Air Live®
Powered by OvisLink Corp.

WH-9200AP

Dual Radio Dual Band
108 Mbps Outdoor AP

User's Manual

www.airlive.com

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product

802.11a/b/g Dual Radio Access Point
AirLive WH-9200AP
is in conformity with

In accordance with 2004/108/ EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause	Description
■**EN 301 893 v1.4.1 (2005-03)**	Broadband Radio Access Network(BRAN); 5GHz high performance RLAN;Harmonized EN Covering essential requirementsArticle 3.2 of the R&TTE Directive.
■ **EN 300 328 v1.7.1 (2005-03)**	Electromagnetic compatibility and Radio spectrum Matters (ERM) Wideband transmission equipment operating in the 2.4GHz ISM band and using spread spectrum modulation techniques; Part 1： technical Characteristics and test conditions Part2：Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive
■ **EN 301 489-1 V1.6.1 (2005-09)** ■ **EN 301 489-17 V1.2.1 (2002-08)**	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and Services; Part 17：Specific conditions for wideband data and HIPERLAN equipment
■ **EN 50385:2002**	Product standard to demonstrate the Compliance of radio base stations and Fixed terminal stations for wireless Telecommunication System with the Basic restrictions or the reference levels related to human exposure to radio Frequency electromagnetic fields (110 MHz -40MHz) - General public
■ **EN 60950-1:2001/A11 :2004**	Safety for information technology equipment including electrical business equipment
■ **CE marking**	CE

Manufacturer/Importer

Signature ： Albert Yeh

Name ： **Albert Yeh**

Position/ Title： **Vice President** (Stamp) Date： **2008/10/17**

AirLive WH-9200AP CE Declaration Statement

Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive WH-9200AP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive WH-9200AP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät AirLive WH-9200AP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive WH-9200AP vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, OvisLink Corp., declares that this AirLive WH-9200AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive WH-9200AP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive WH-9200AP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive WH-9200AP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive WH-9200AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive WH-9200AP atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive WH-9200AP står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Country	Declaration
lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive WH-9200AP atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel AirLive WH-9200AP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive WH-9200AP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive WH-9200AP megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive WH-9200AP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	OvisLink Corp declara que este AirLive WH-9200AP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive WH-9200AP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive WH-9200AP spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive WH-9200AP tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive WH-9200AP er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
no Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive WH-9200AP er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the written consent of OvisLink Corp.
Windows™ 95/98 and Windows™ 2000 are trademarks of Microsoft® Corp.

Pentium is trademark of Intel.

All copyright reserved.

Table of Contents

1. Introduction 5

1.1 Overview 5

1.2 Installing WH-9200AP 6

1.2.1 Package Content 6

1.2.2 Hardware Presentation 7

1.2.3 Configuration Setups 11

2. Operation Mode 13

2.0 Change Operation Mode 14

2.1 Dual AP Mode 15

2.3 Dual WDS Bridge Mode 19

2.4 Separate Bridge Mode 21

2.5 AP + Client / Client + AP Mode 23

2.6 AP + WDS Bridge / WDS Bridge + AP Mode 25

2.7 WDS + Gateway / Gateway + WDS Mode 27

2.8 AP + Gateway / Gateway + AP Mode 29

2.9 AP + WISP / WISP + AP Mode 31

3. Wireless Settings 33

3.1 Access Point Mode 33

3.2 WDS Bridge Mode 35

3.3 Client Mode 37

3.4 Gateway (AP Router) Mode 40

3.4.1 WAN Port Settings 41

3.4.2 DHCP Server Settings 42

3.4.3 DMZ & Virtual Server 43

3.4.4 IP Filter Settings 44

3.4.5 IP Routing Settings 47

3.4.6 Dynamic DNS (DDNS) Settings 48

3.5 WISP Mode 49

3.6 Wireless Security 51

3.7 Advanced Wireless Settings 59

3.8 Access Control 62
3.9 Bandwidth Control 63
3.9.1 Total Bandwidth Control 64
3.9.2 Per user Bandwidth Control 66
3.10 Multiple SSID + VLAN 67
4. System Management 68
4.1 Change Password 68
4.2 System Management Settings 69
4.3 SNMP Settings 71
4.4 Firmware Upgrade 73
4.5 Configuration Save and Restore 74
4.6 Factory Default ..... 錯誤! 尚未定義書籤。
4.7 Reboot System 75
4.7 Reboot System 75
4.8 WH-9200AP Emergency Recovery 76

1. Introduction

1.1 Overview

The WH-9200AP is a dream device for WISP to build their wireless networks. The AP features 2 Atheros 11a/b/g radios that run in 5GHz or 2.4GHz frequency band. Moreover, it provides hi-power at 11a mode for extra long distance application. There is an intergraded 802.3af POE port to let you run the AP at up to 100 meter distance away from the power source.

Dual Wireless + Hi Power + 2 LAN Ports

The WH-9200AP is equipped with 2 high-powered Atheros radios. The radio 1 runs in the 11a 5GHz mode only while the radio 2 runs at the 11a/b/g dual band mode. AirLive adds high power amplifier to run the AP at 23dBm in 11a mode (200mW), that's 4 times the output power of normal 11a radio (50mW). In addition, 2 programmable LAN ports are available for multi-mode AP/Gateway configuration.

Multiple Operation Modes

The WH-9200AP can operate in multiple wireless modes for different application environments such as Dual AP, Dual WDS, Duplex link aggregation, Separate Bridge, AP + Client, AP + WDS, WDS + Gateway, AP + Gateway, and AP + WISP. These modes can be changed and configured easily by the Web user interface.

802.3af PoE Port

WH-9200AP is equipped with an 802.3af Power over Ethernet port. It thus can be powered by a PoE PSE and operate at up to 100 meter away.

VLAN & QoS

WH-9200AP provides Multi-SSID to create different wireless networks using one AP. The TAG VLAN feature allows service provider to control service content of each SSID network all the way back to core router. The QoS feature allows prioritizing the different package according the 802.11e WMM protocol and triple play (Voice, Video and Data). Bandwidth control feature allow WH-9200AP to limit the bandwidth on distinct IP/MAC or on the total device.

IP67 Environmental Protection Enclosure

With IP-67 industrial standard enclosure, WH-9200AP is highly protected against dust and water. So that WH-9200AP can be used in a hardened environment.

1.2 Installing WH-9200AP

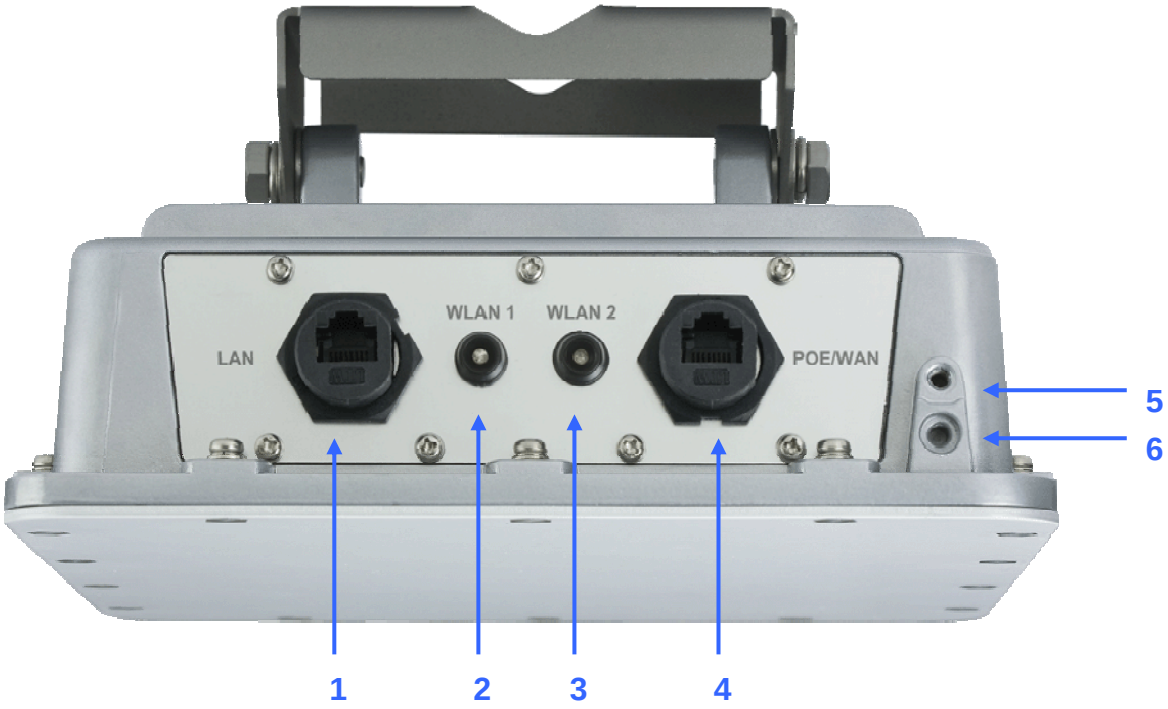
This section describes the installation procedure for the WH-9200AP. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the WH-9200AP. Finally, this section explains how to configure a Windows PC to communicate with the WH-9200AP.

1.2.1 Package Content

The WH-9200AP package contains the following items:

- One WH-9200AP main unit
- 48VDC PoE injector kits
- Pole/Wall mount kit
- One CD of the WH-9200AP
- Quick Start Guide

1.2.2 Hardware Presentation



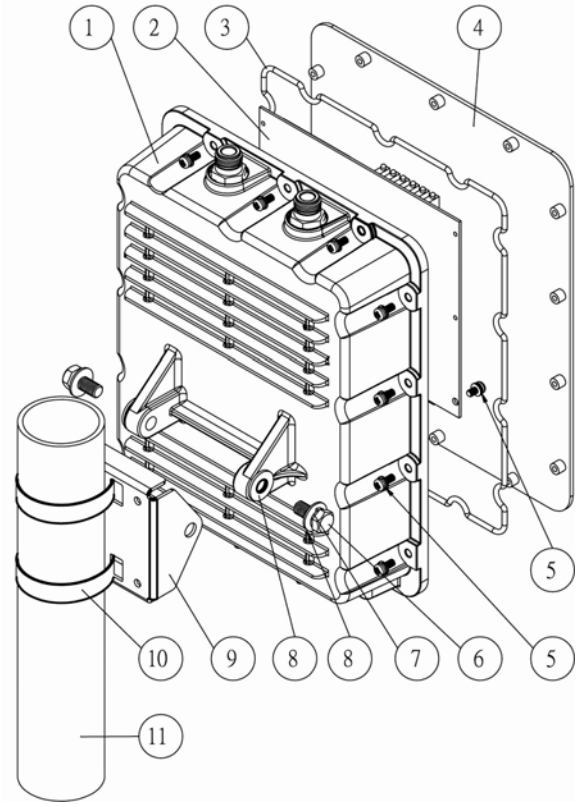
LED #	Function	Color	Description
1	LAN	-	LAN port #2
2	WLAN1 LED	Blue	No Connection: Off Low Signal: Flash per second Better Signal: Flash every 2 seconds Best Signal: Steady On
3	WLAN2 LED	Green	
4	POE/WAN	-	LAN port #1, compatible with 802.3af PoE. Become WLAN port when operate in Gateway mode
5	Ground Pin	-	Reference point for electric current
6	Sluice	-	Sluice out the water in device

N-Type connector for outdoor antenna of Radio 1
N-Type connector for outdoor antenna of Radio 2
Air Live
Antenna 1
Antenna 2

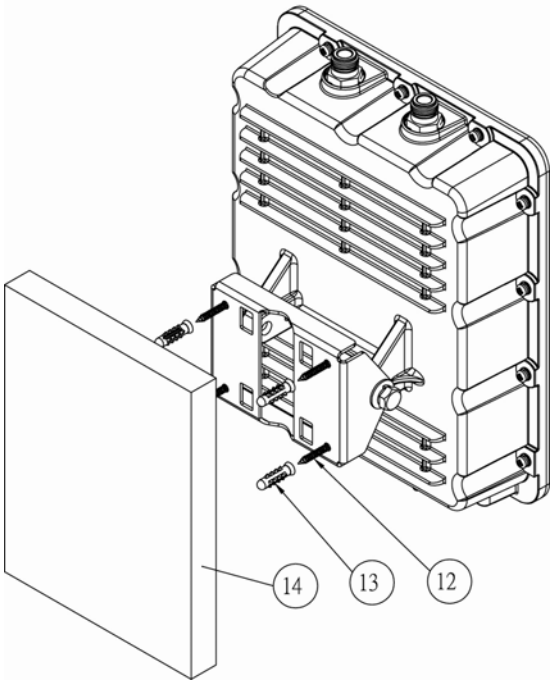
Pole Mount/Wall mount Installation

①	Enclosure assembly	- 1 set
②	PCB assembly	- 1 set
③	Gasket of front cover	- 1 pc
④	Front cover	- 1 pc
⑤	M4-10 screw	- 16 pcs
⑥	M8-20 screw	- 2 pcs
⑦	M8 spring washer	- 2 pcs
⑧	M8 washer	- 4 pcs
⑨	Mounting	- 1 pc
⑩	Pole clamp	- 2 pcs
⑪	POLE(MAX.:2 inch)	
⑫	Wall screw	- 4 pcs
⑬	Plastic anchor	- 4 pcs
⑭	Wall	

Pole Mount

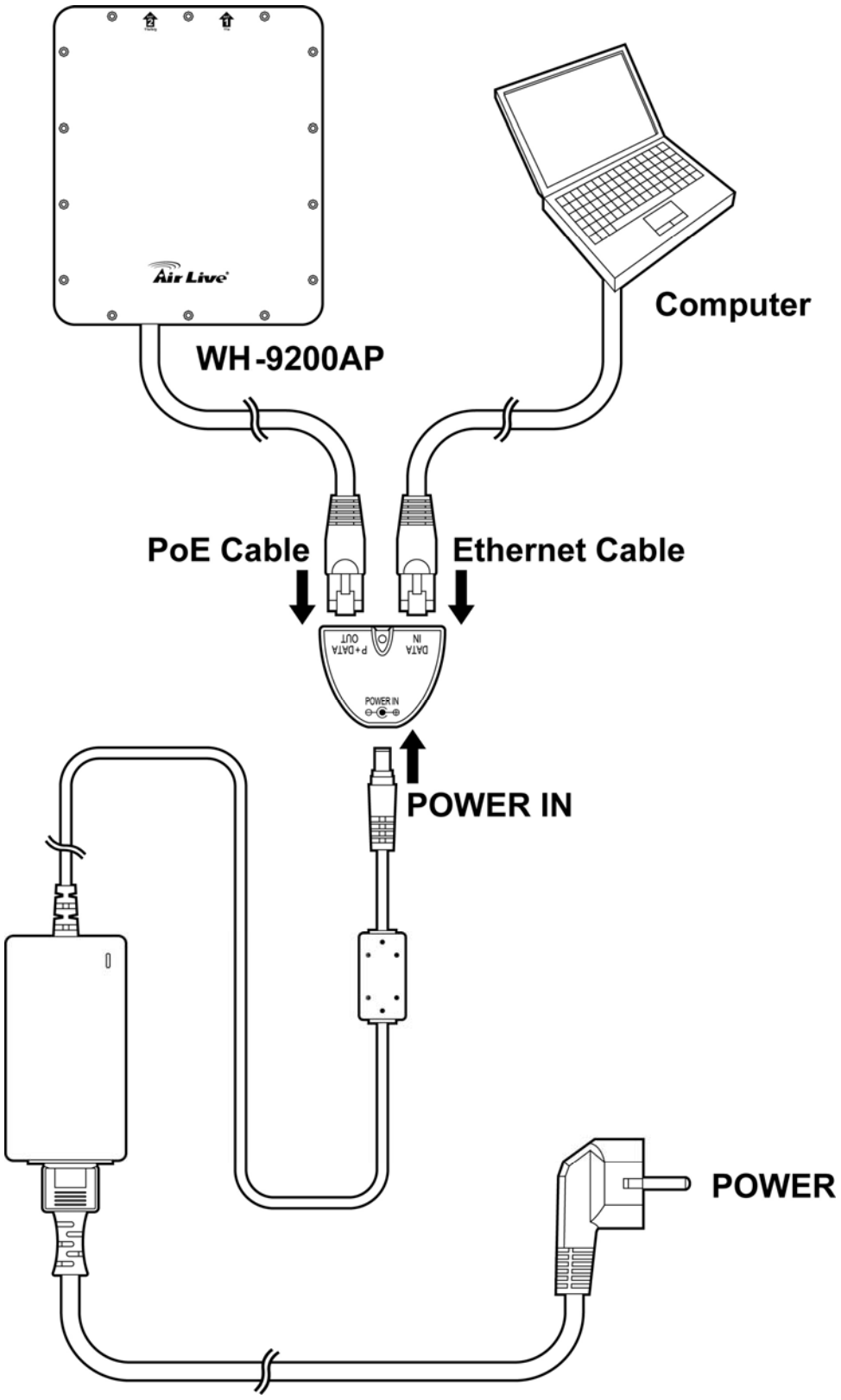


Wall Mount



Power Installation

The following image shows the power installation of WH-9200AP. Note that WH-9200AP is IEEE802.3af compatible, you should use the packed POE kit or POE switch for power injection.



1.2.3 Configuration Setups

The factory default settings of WH-9200AP are as following:

Settings	Default Value	
	Wireless1	**Wireless2**
Device Name	WH-9200AP	
Radio	802.11a	802.11a
SSID	airlive1	airlive2
Channel	36	36 (auto in 802.11b/g)
WEP	Disabled	
IP Address	192.168.1.1	
DHCP Server	Disabled. Available and default enabled when each of the wireless is configured as a gateway.	
DHCP IP Range	192.168.1.2 ~ 192.168.1.254	
Access Password	airlive	

Note: Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations. Also, remember to adjust the antenna; usually the higher the antenna is placed; the better will be the performance.

1. Connect to your local area network: connect an Ethernet cable to one of the Ethernet port.
2. (LAN1, LAN2) of this Wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.
3. Power on the device: connect the included AC power adapter to the Wireless Access Point's power port and the other end to a wall outlet.

Access to management interface

1 Please make sure your computer IP is in the same subnet as the AP (i.e. 192.168.1.x).

2 Please make sure your computer has wireless network adapter installed.

3 Open the web browser and enter http://192.168.1.1/.

Air Live
WH-9200AP
Dual Radio Dual Band Outdoor Access Point
www.airlive.com
Wireless Settings
Configure the Operation Mode of your WH-9200AP
System Configuration
Change the password, upgrade the firmware, reboot the Wireless Access Point, and more.
Device Status
Show the device information, syslog table, wireless client table, and more.
Help
Get help with commonty asked questions about the Wireless Access Point.

4. Connect Wireless Settings to start.

2. Operation Mode

The WH-9200AP device provides all 14 modes of wireless operational applications with:

Mode	Radio 1 (11a)	Radio 2 (11a/b/g)
Dual AP	Access Point	Access Point
Duplex	WDS Bridge	WDS Bridge
Dual WDS Bridge	WDS Bridge	WDS Bridge
Separate Bridge	WDS Bridge	WDS Bridge
AP + Client	Access Point	Wireless Client
Client + AP	Wireless Client	Access Point
AP + WDS Bridge	Access Point	WDS Bridge
WDS Bridge + AP	WDS Bridge	Access Point
WDS + Gateway	WDS Bridge	Gateway (AP Router)
Gateway + WDS	Gateway (AP Router)	WDS Bridge
AP + Gateway	Access Point	Gateway (AP Router)
Gateway + AP	Gateway (AP Router)	Access Point
AP + WISP	AP Router	WISP Bridge
WISP + AP	WISP mode	AP Router

2.0 Change Operation Mode

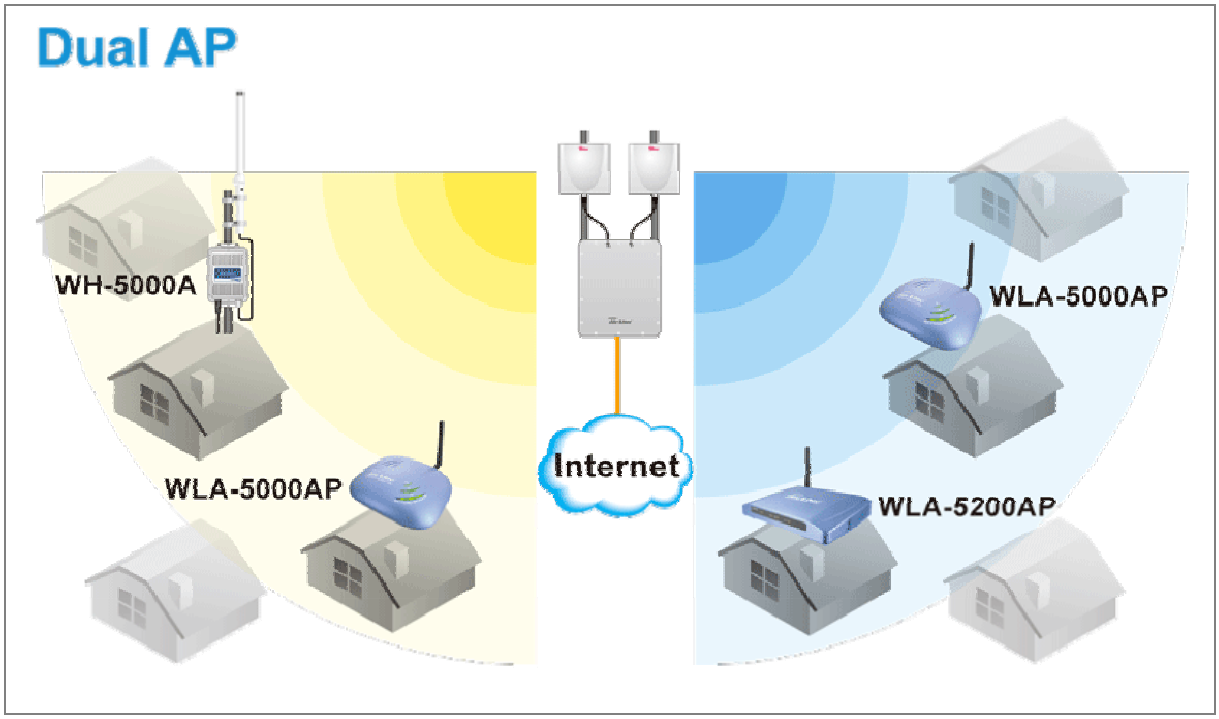
WH-9200AP is default in Dual AP mode. If the mode had been changed, click the **“Operation Mode”** button to change back.

To change operation Mode:

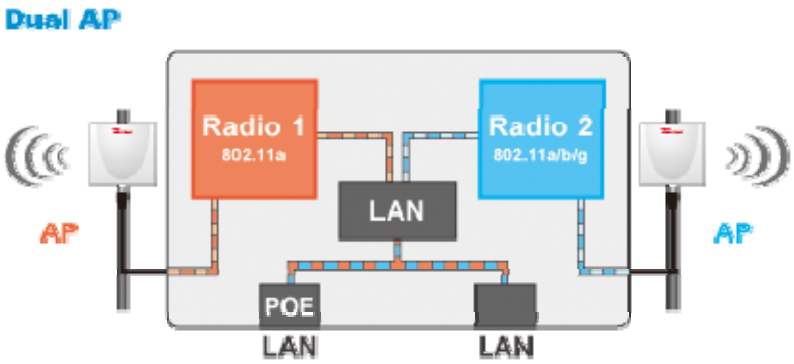
1. Click on **“Operation Mode“**
2. Select Operation Mode in the main page
3. Click “Change Mode” button to apply
4. The device reboot to select mode

2.1 Dual AP Mode

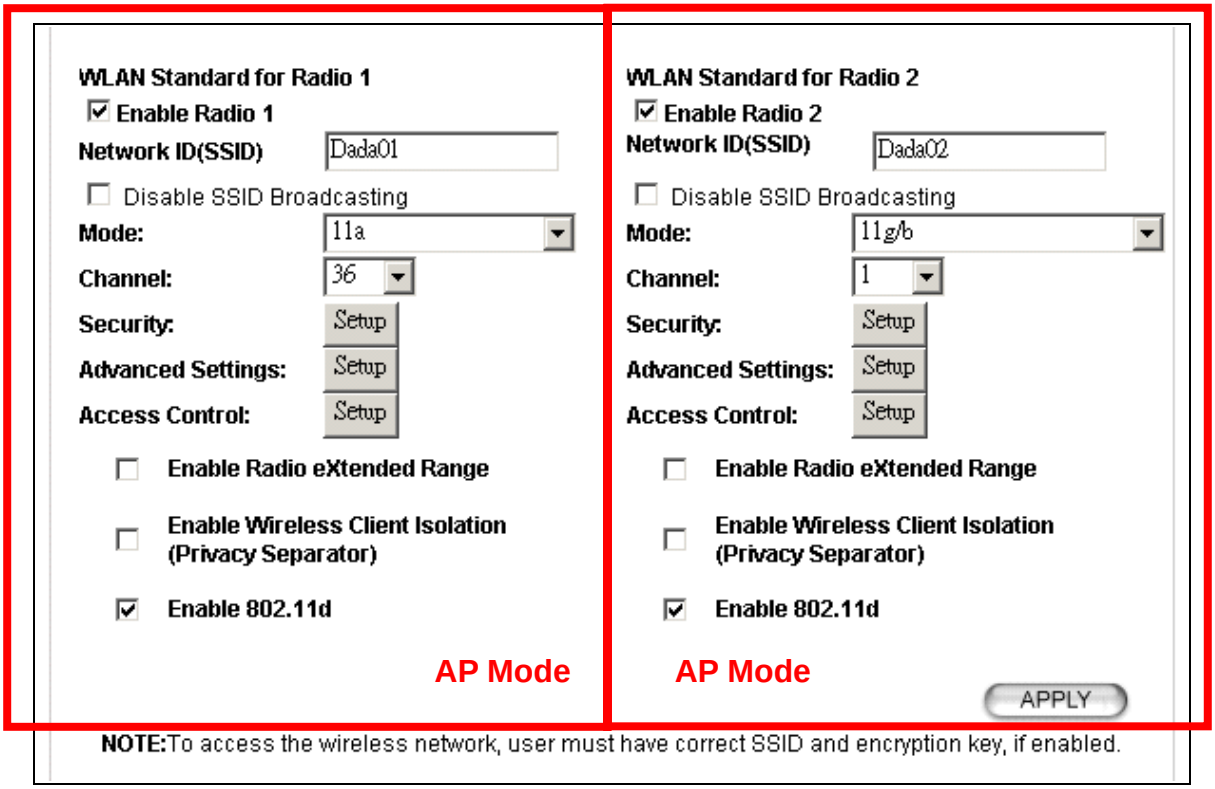
In Dual AP mode, both wireless interface of WH-9200AP are set as AP and provide hotspot service on each interface.



- This Application provides wider coverage that difficult to be reached with a unique Omni antenna by using another adequate antenna such as sector antenna. It's particularly suitable for WISP to provide stable and high performance link.
- The image in Dual AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



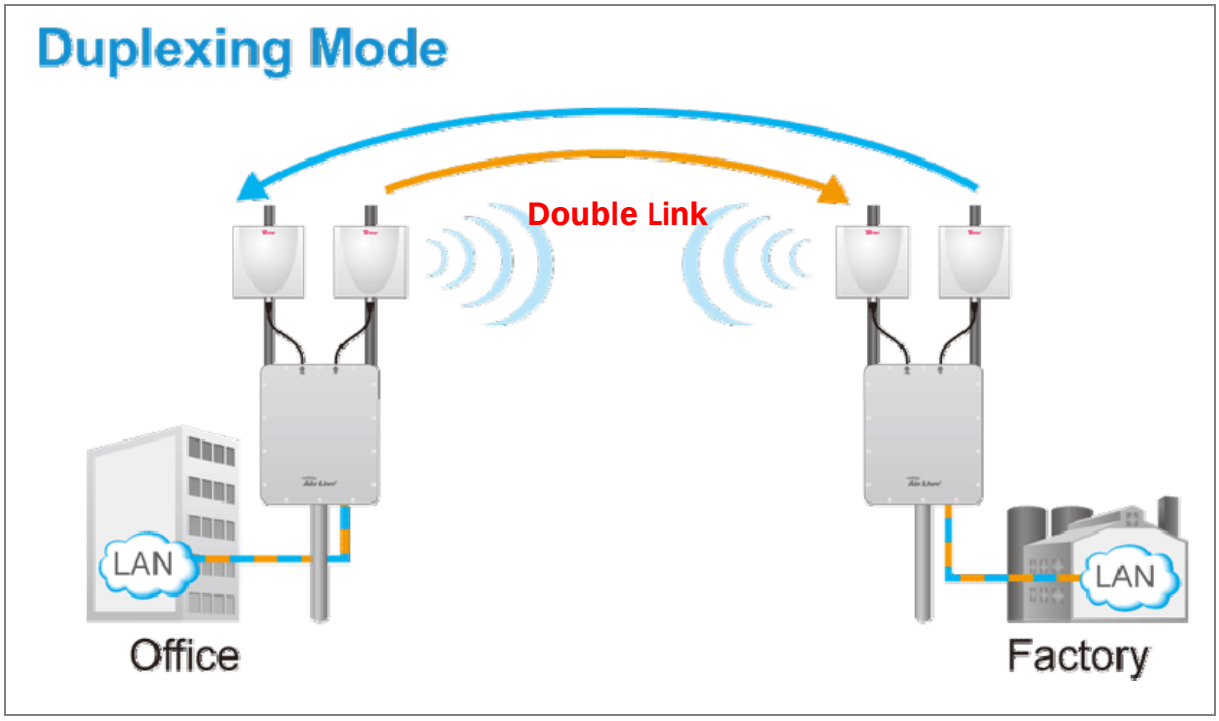
Both Radios has its own setting interface.



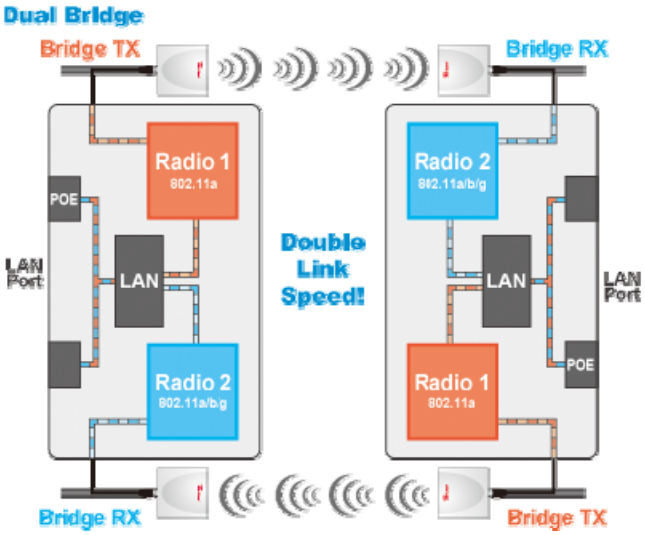
To configure AP mode, please refer to Section 3.1 Access Point Mode.

2.2 Duplex Mode

The duplex mode groups the two radios to double the bandwidth between two WH-9200APs.



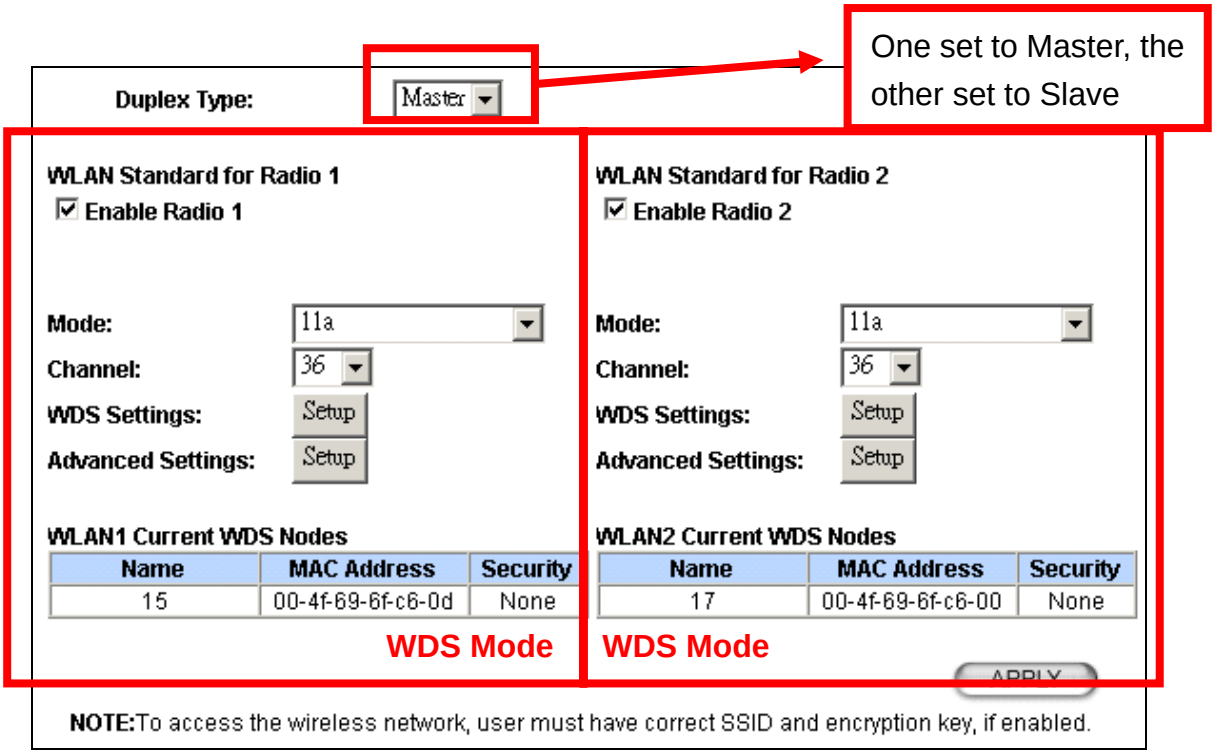
- This Application provides higher bandwidth between two locations than single radio does. When clients transmitting data which over the loading of single radio, the other radio shares the loading and make it able to transmit more data between the two WH-9200AP.



- The image in Duplex mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.

Both radios are using WDS mode for communication.

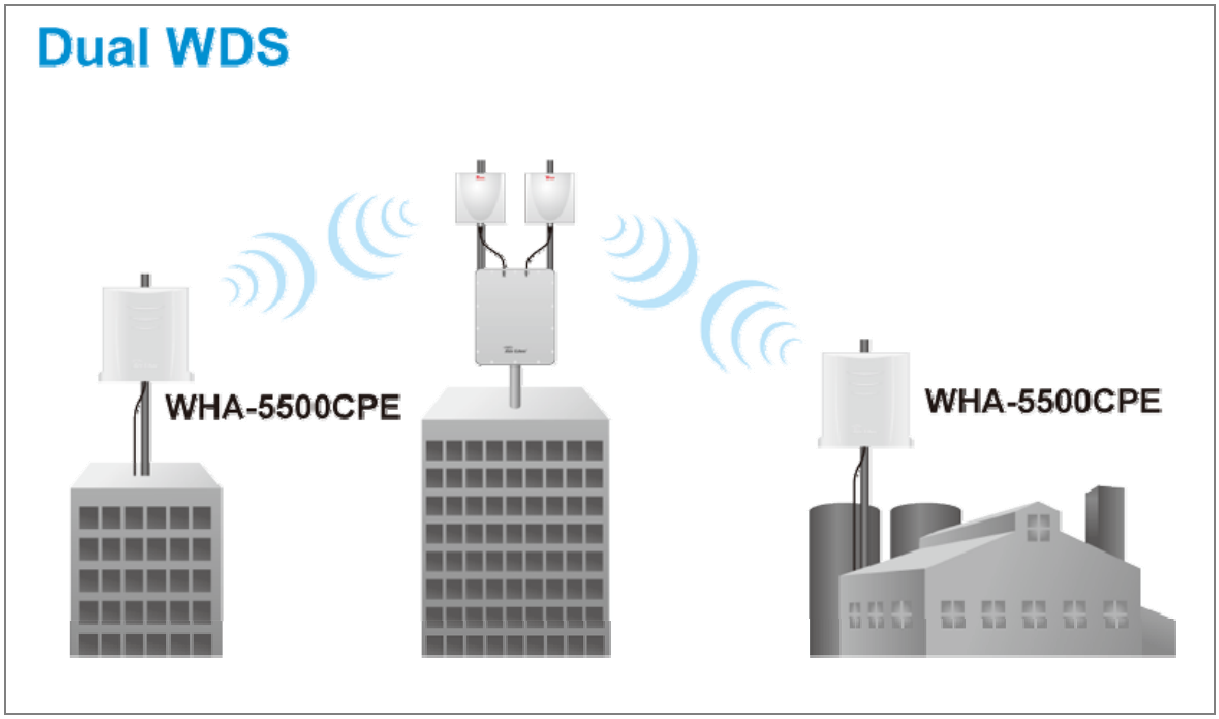
One WH-9200AP is configured as a Master where as the other WH-9200AP is configure to be a Slave.



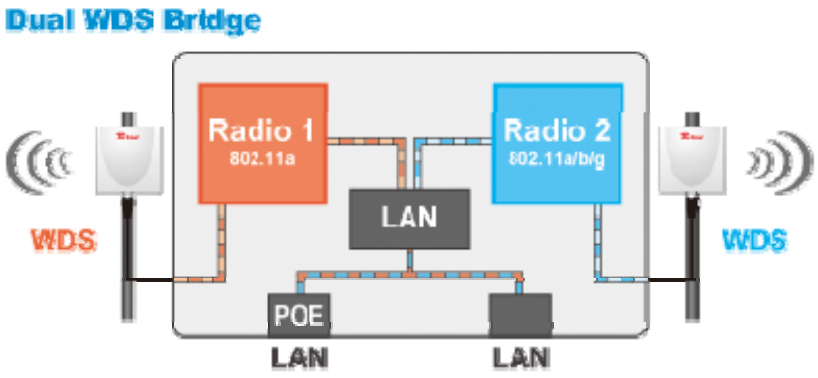
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

2.3 Dual WDS Bridge Mode

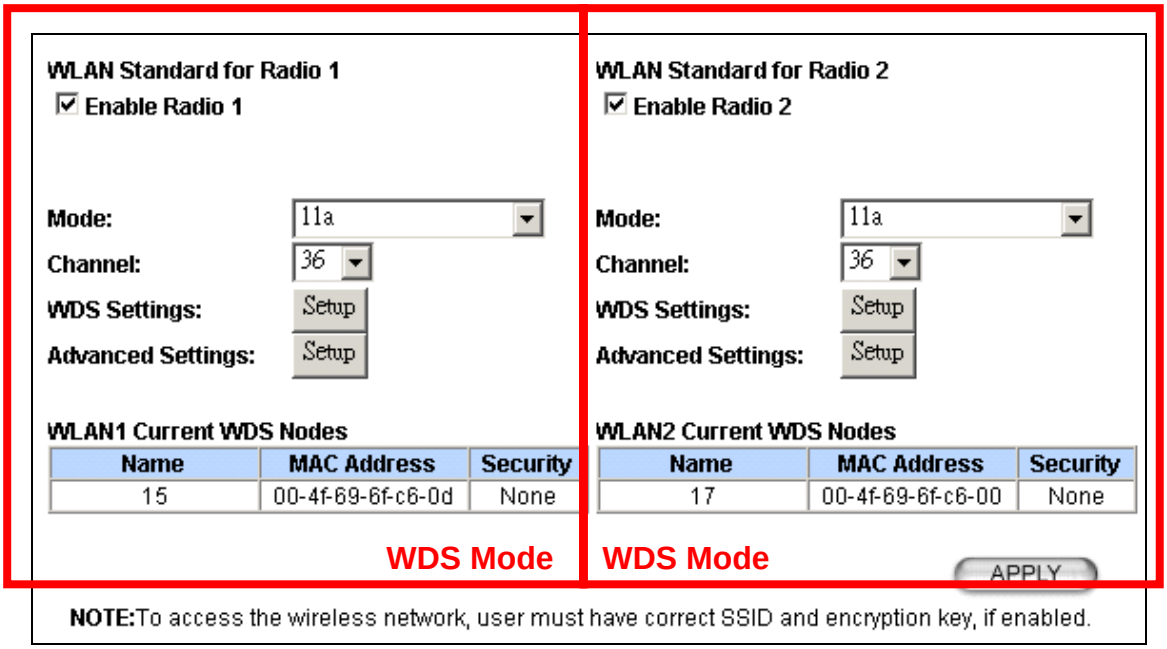
In Dual WDS Bridge mode, both wireless interface of WH-9200AP are set as WDS Bridge and connect to remote network. When configured in the Dual WDS Bridge mode, a WH-9200AP allows solving discontinuous link due to geographical obstacles, shown as below and extension of distance between two WDS bridge nodes separated by a building.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in Duplex WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



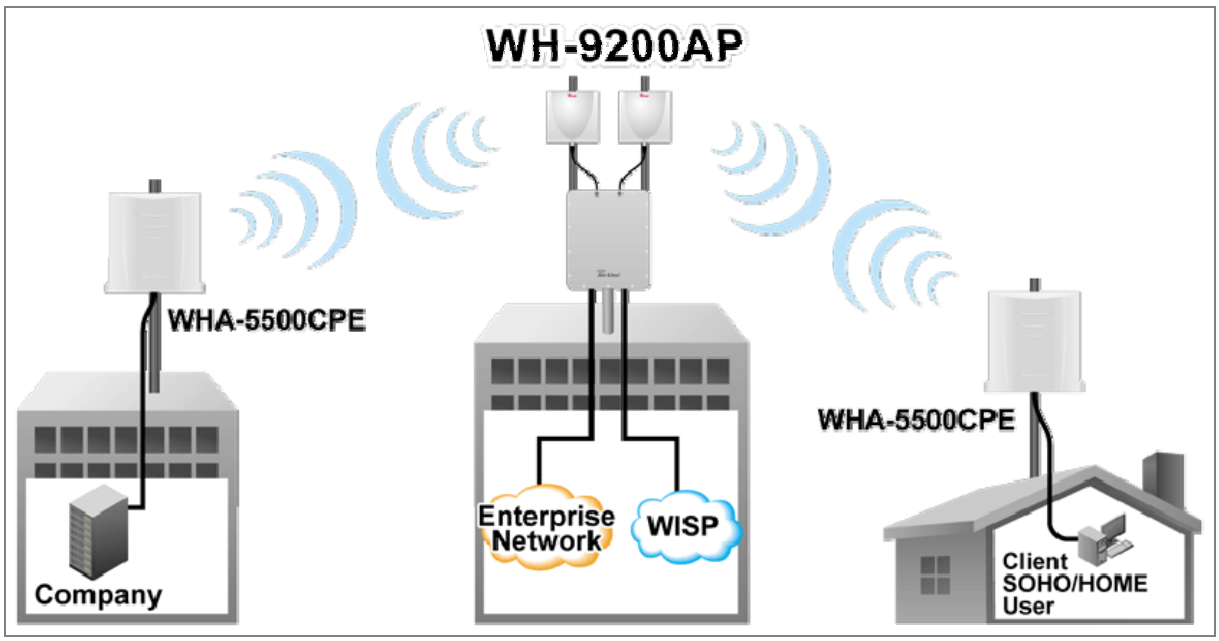
Both radios are using WDS mode for communication.



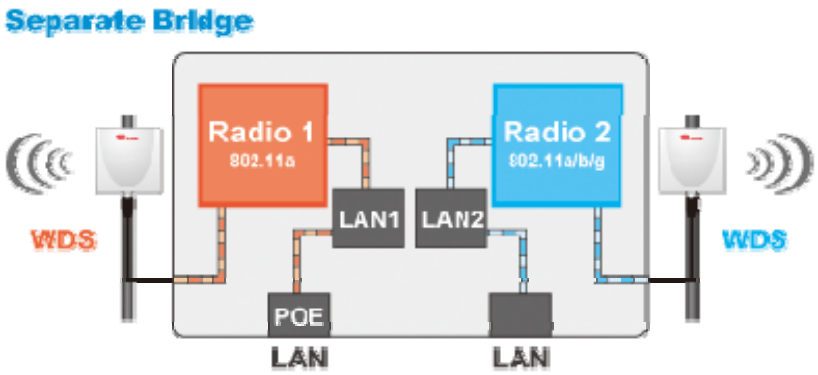
To configure the WDS mode please refer to section 3.2 WDS Bridge Mode ……

2.4 Separate Bridge Mode

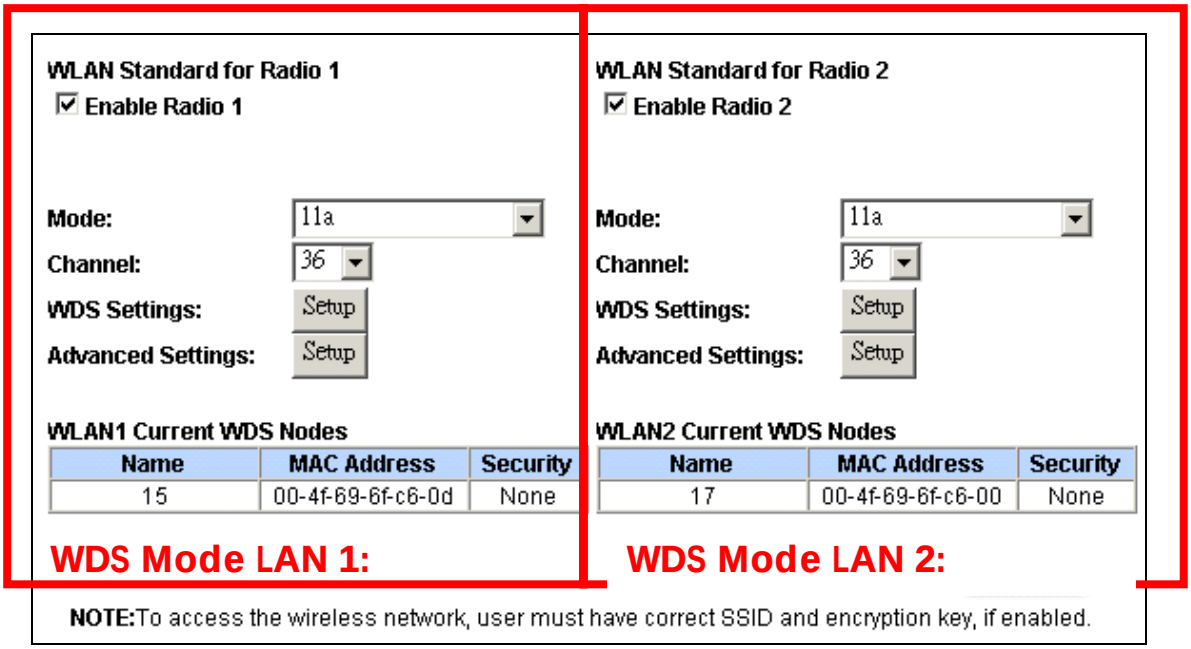
The Separate Bridge separates the device into 2 IP segments. Radio 1 and LAN 3 are in IP segment of 192.168.1.x/24 and Radio 2 and LAN1, LAN2 are in IP segment of 192.168.2.x. Devices in one IP segment can not communicate to devices in the other IP segment.



- In this application, both Radio 1 and Radio 2 are in WDS Bridge Mode.
- The image in Separate WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



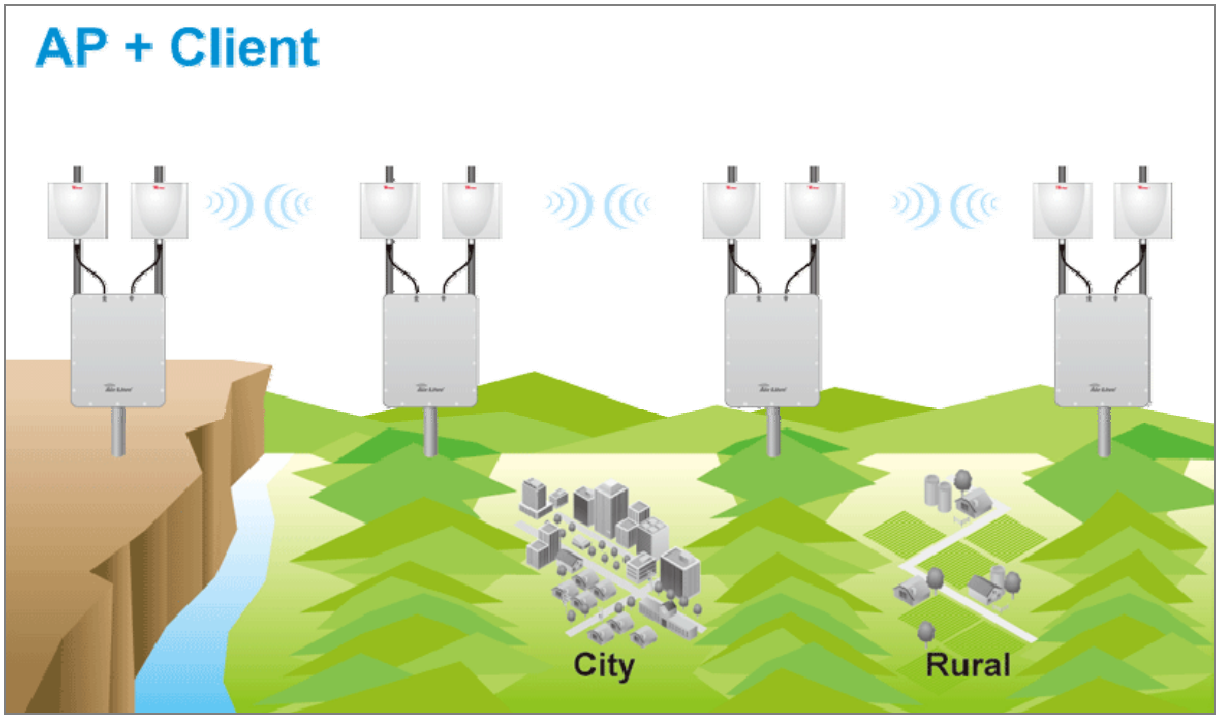
Both radios are using WDS mode for communication.



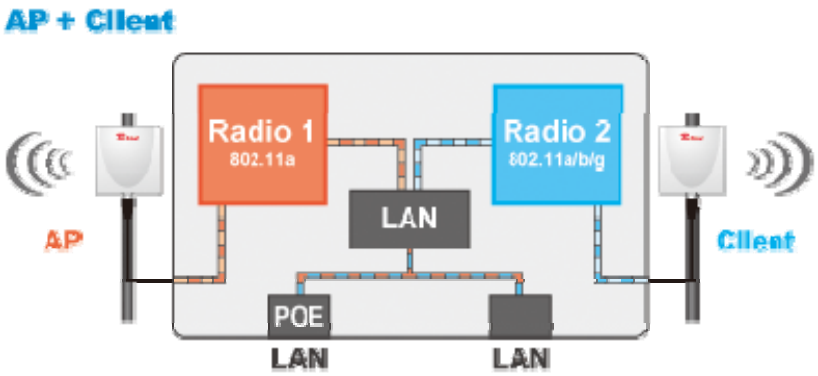
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode……

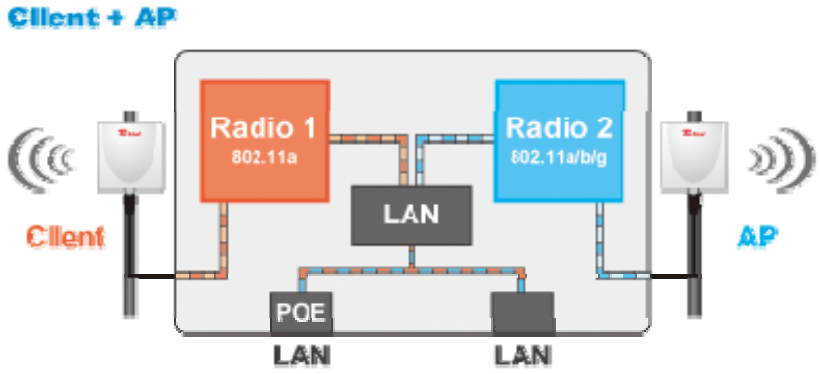
2.5 AP + Client / Client + AP Mode

In this mode, one station works as an intermediate station. This enable the AP to link with remote stations using client mode, then distribute the signal to other clients using AP mode.

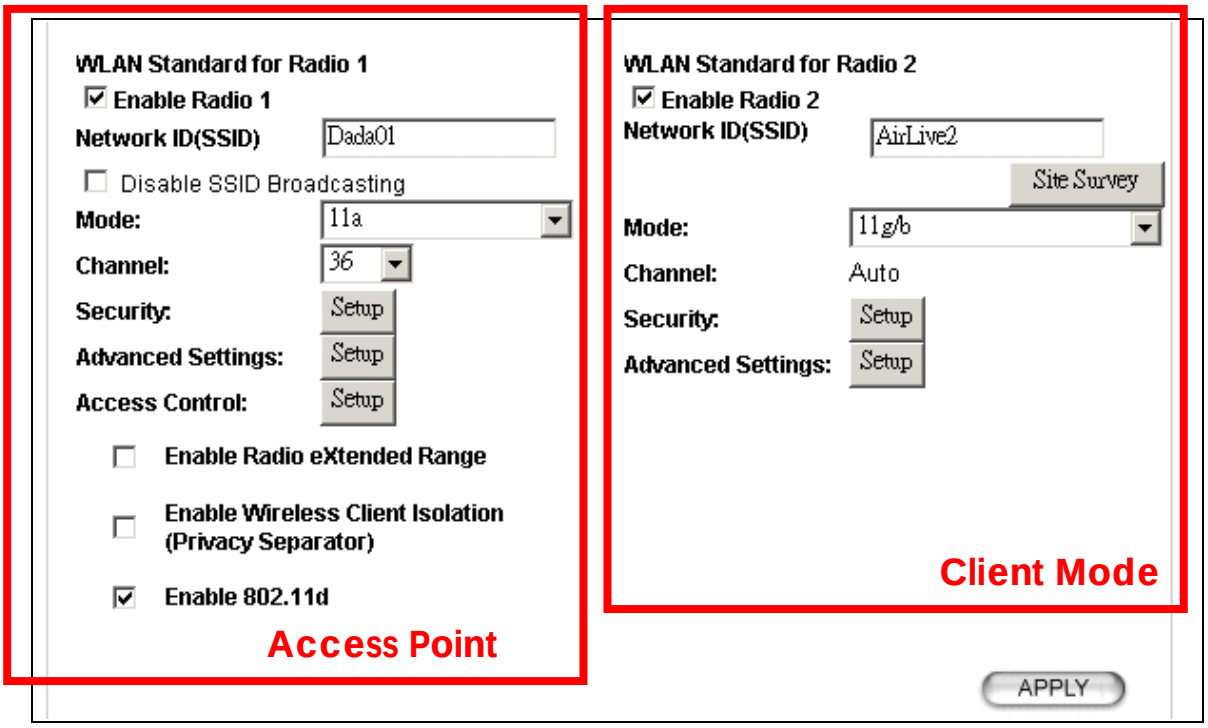


- In this application, Either Radio 1 or Radio 2 is in AP Mode, the other Radio is in Client mode.
- The image in AP + Client / Client + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + Client is as following:

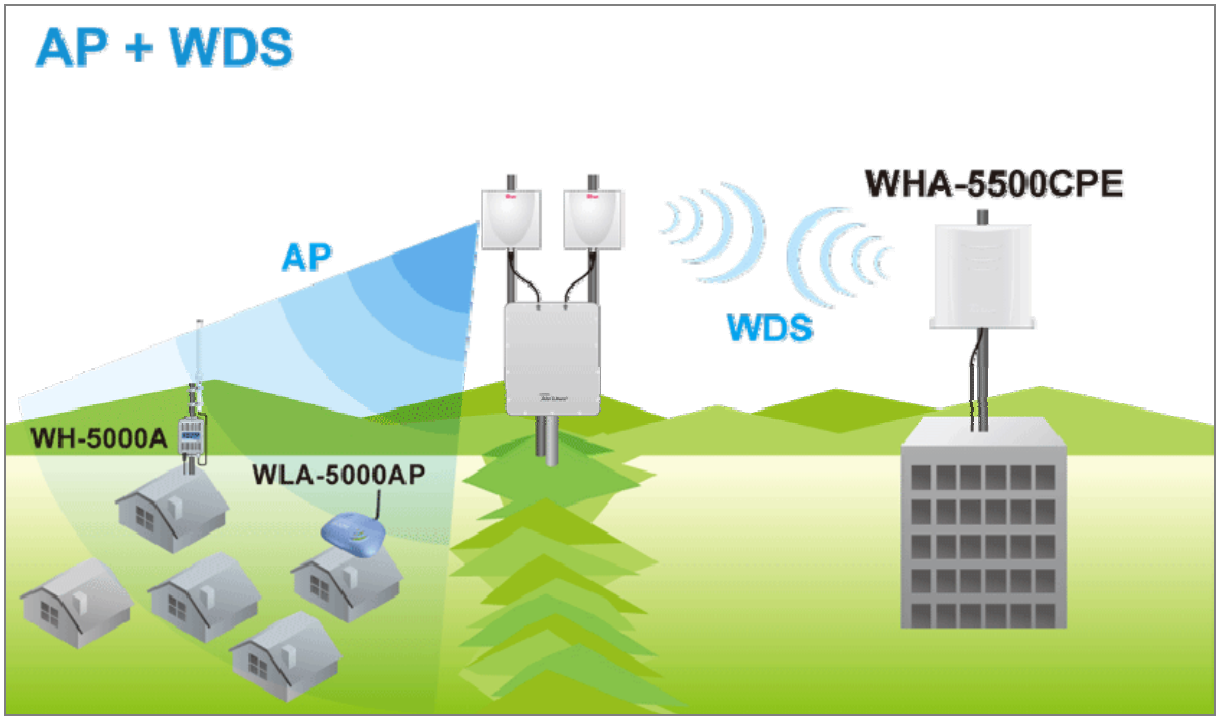


To configure the AP mode, please refer to Section 3.1 Access Point Mode……

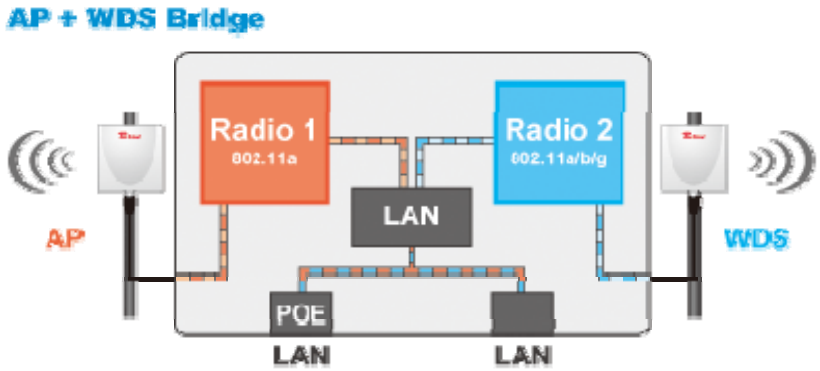
To configure the Client mode, please refer to Section 3.3 Client Mode ……

2.6 AP + WDS Bridge / WDS Bridge + AP Mode

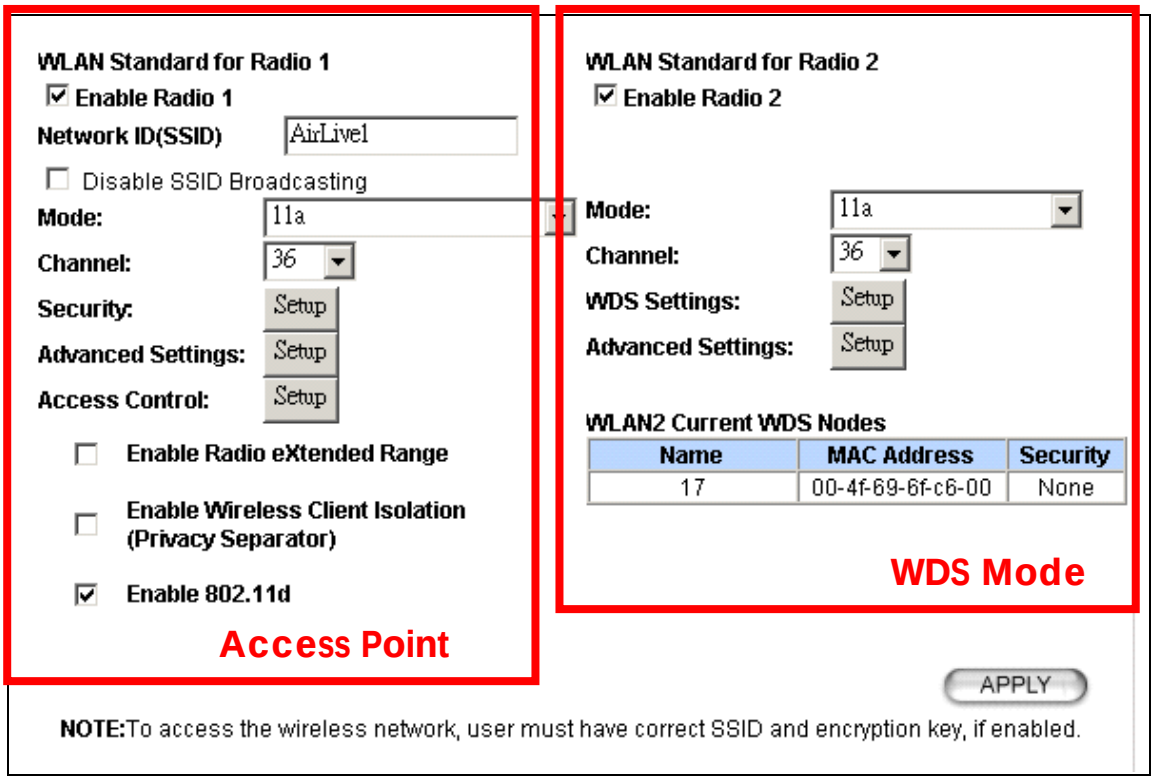
In this mode, one Radio is in Access Point mode and the other in WDS Bridge Mode.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in AP + WDS Bridge / WDS Bridge + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



The UI example of AP + WDS Bridge is as following:

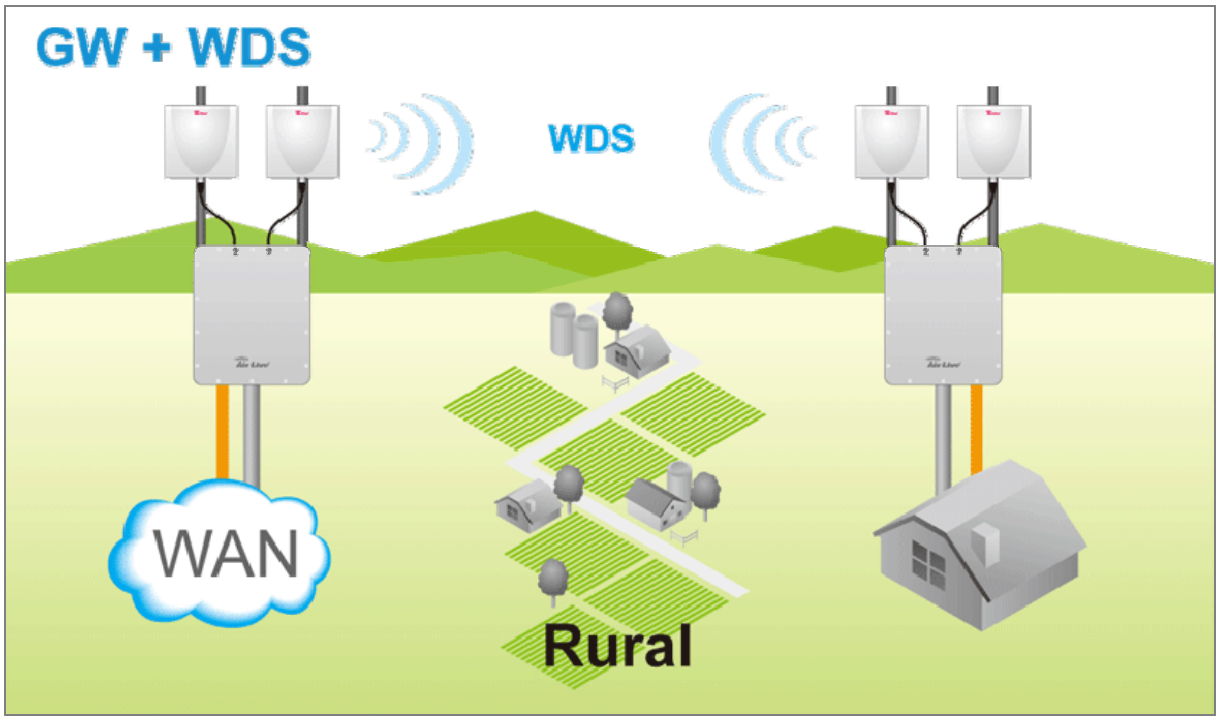


To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

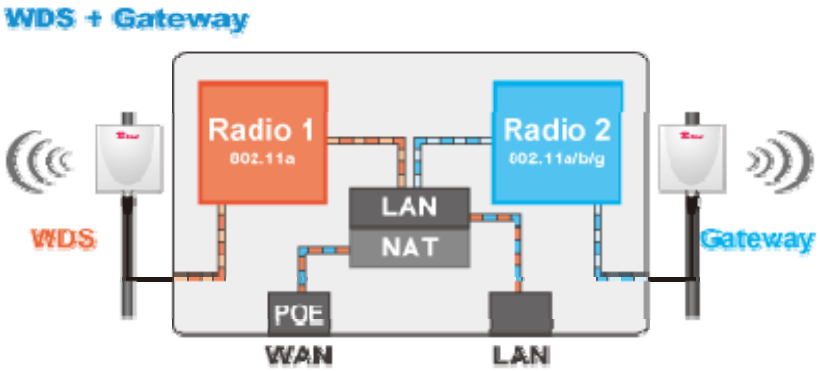
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

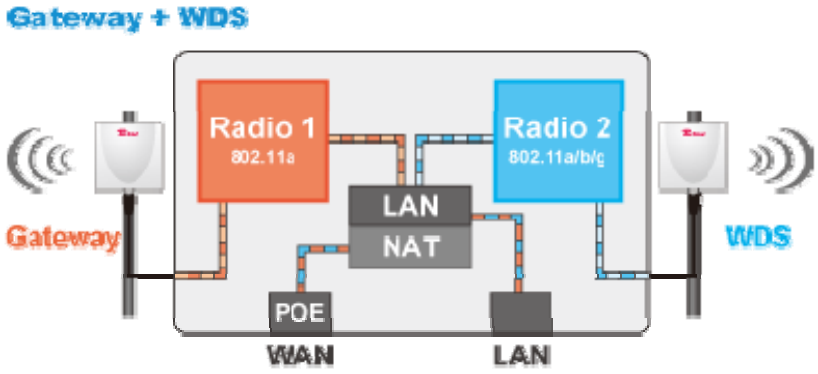
2.7 WDS + Gateway / Gateway + WDS Mode

In this mode, one radio acts as an AP router and the other a WDS bridge. One of the RJ-45 ports as the WAN interface to the internet.

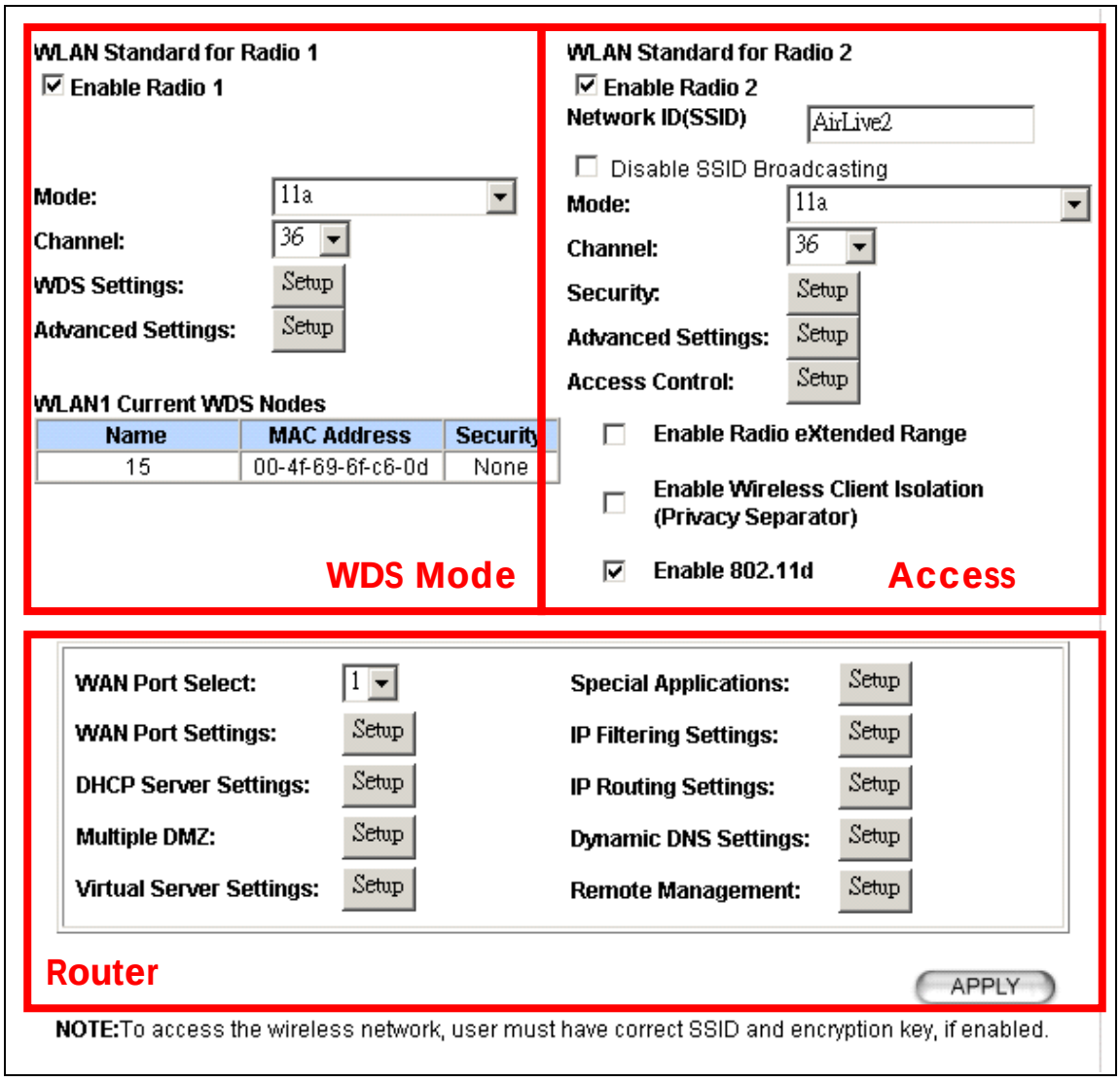


- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in WDS + Gateway / Gateway + WDS mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + WDS Bridge is as following:



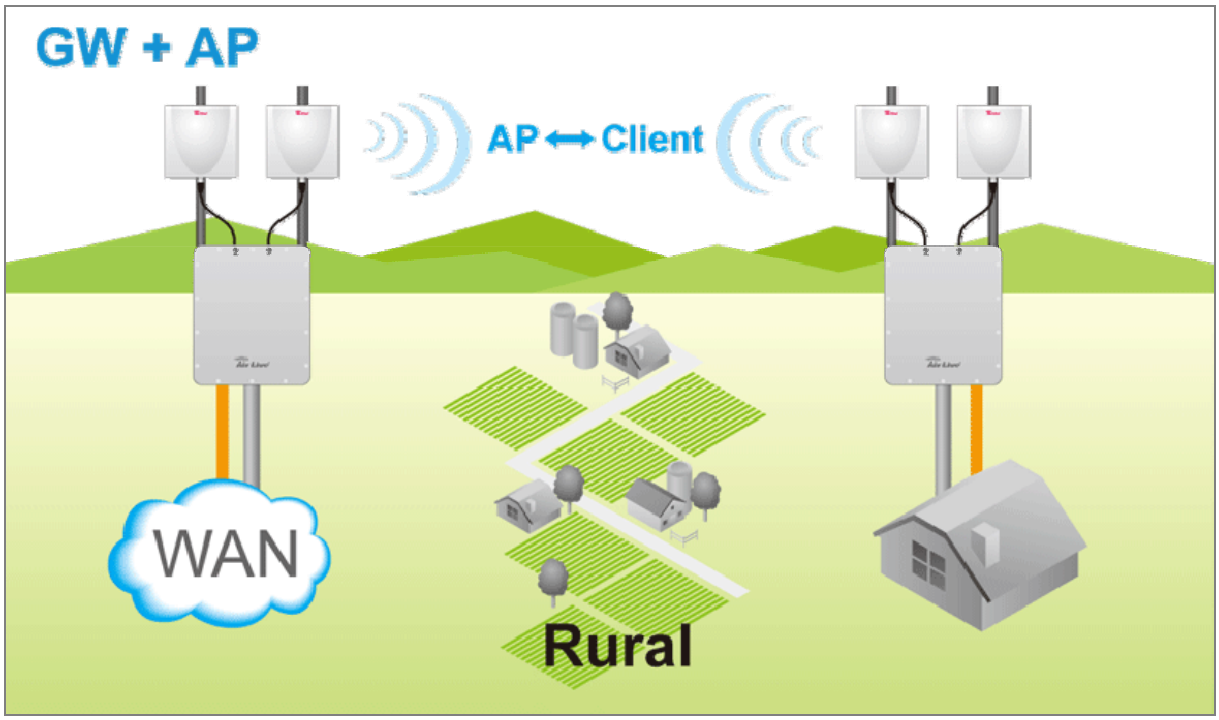
To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

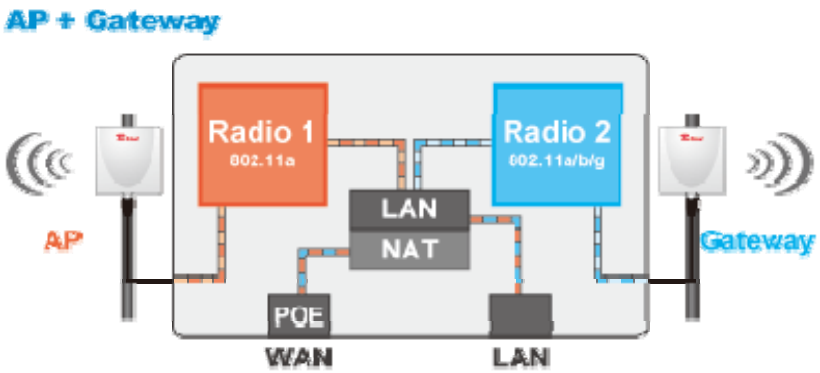
To configure the Gateway (Router) mode. Please refer to Section 3.4 Gateway Mode ……

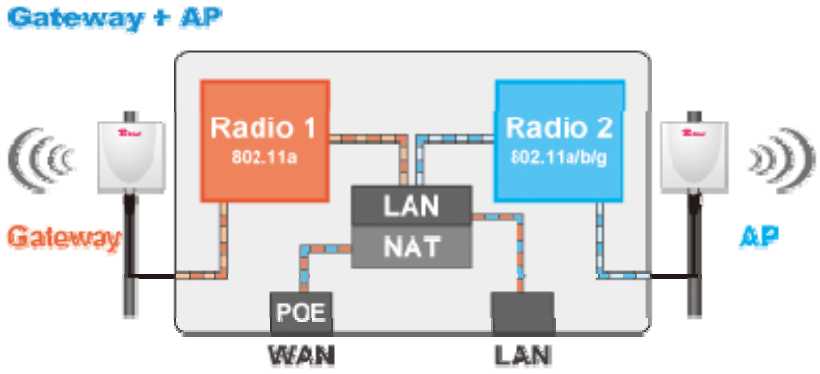
2.8 AP + Gateway / Gateway + AP Mode

In this mode, one radio acts as an AP router and the other an Access Point. One of the RJ-45 ports as the WAN interface to the internet.



- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + Gateway / Gateway + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





WLAN Standard for Radio 1

Enable Radio 1

Network ID(SSID): AirLive1

Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

Enable Radio eXtended Range

Enable Wireless Client Isolation (Privacy Separator)

Enable 802.11d

AP Mode

WLAN Standard for Radio 2

Enable Radio 2

Network ID(SSID): AirLive2

Disable SSID Broadcasting

Mode: 11a

Channel: 36

Security: Setup

Advanced Settings: Setup

Access Control: Setup

Enable Radio eXtended Range

Enable Wireless Client Isolation (Privacy Separator)

Enable 802.11d

AP Mode

WAN Port Select:	1	Special Applications:	Setup
WAN Port Settings:	Setup	IP Filtering Settings:	Setup
DHCP Server Settings:	Setup	IP Routing Settings:	Setup
Multiple DMZ:	Setup	Dynamic DNS Settings:	Setup
Virtual Server Settings:	Setup	Remote Management:	Setup

Router / WAN

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

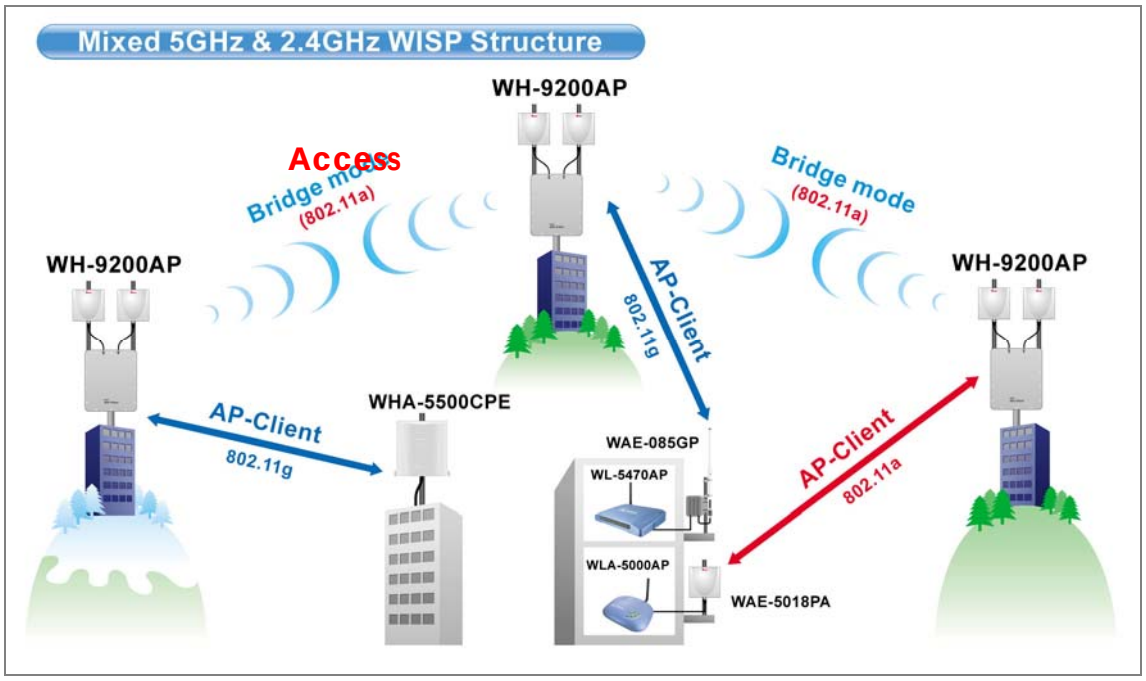
To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

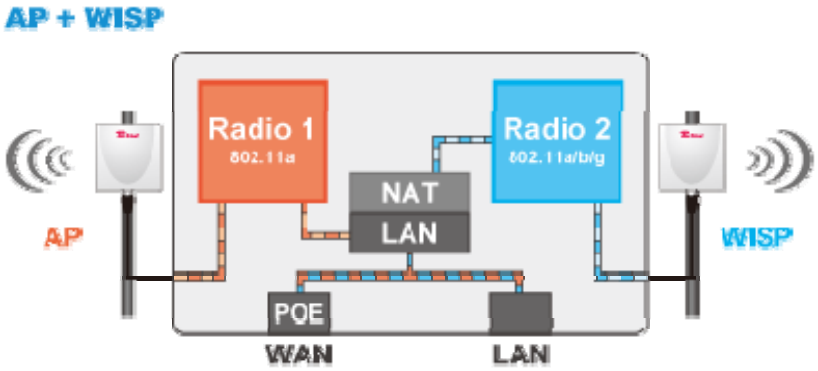
To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

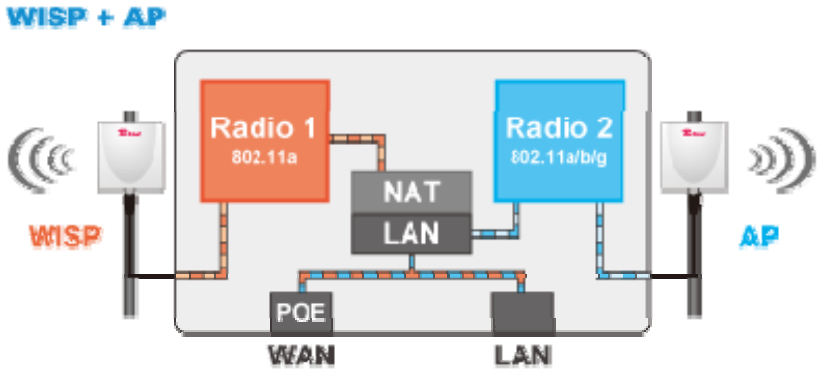
2.9 AP + WISP / WISP + AP Mode

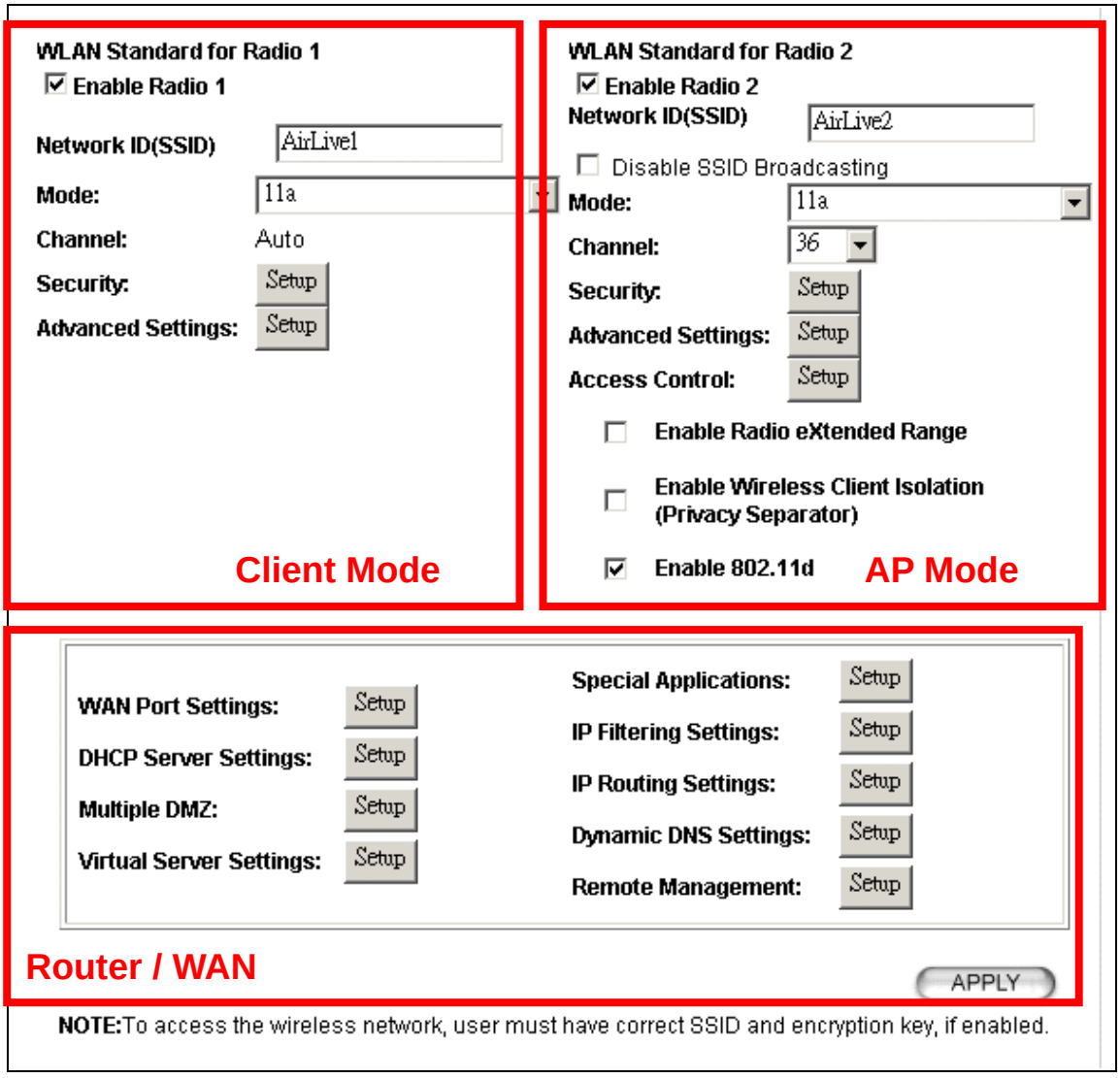
In this mode, one radio acts as an AP and the other an client router. One of the RJ-45 ports as the WAN interface to the internet.



- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + Gateway / Gateway + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.







To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the Client mode, Please refer to Section 3.3 Client Mode ……

To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

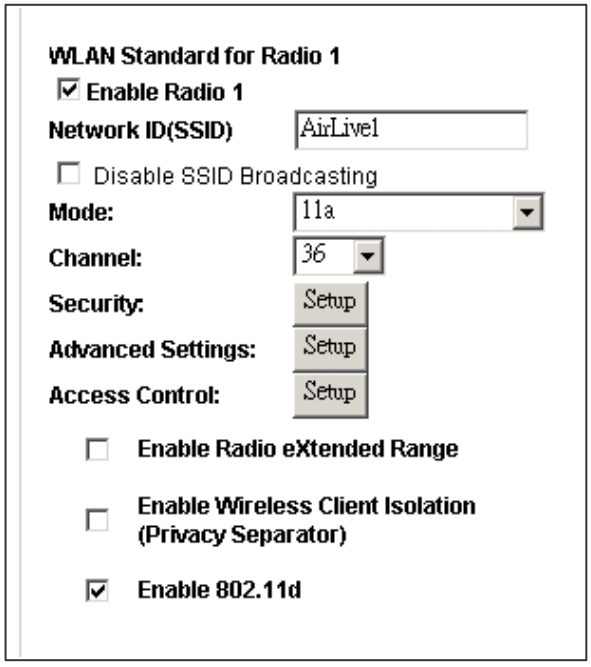
3. Wireless Settings

This section guides you to configure the mode of the Radio interface. Note that the radio can select either 11a or 11b/g mode.

3.1 Access Point Mode

The Access Point mode is the most basic mode of multi-function Access Point. In this mode, the AP will act as a central hub for different Wireless LAN clients. Some hotspot Access Points requires 802.1x authenticator function to authenticate a user before providing internet service.

Access Point mode included in these operation modes: Dual AP, AP + Client, Client + AP, AP + WDS Bridge, WDS Bridge + AP, AP + Gateway, Gateway + AP, AP + WISP and WISP + AP modes.
Enable Radio: Use this check box to turn on or turn off the radio.



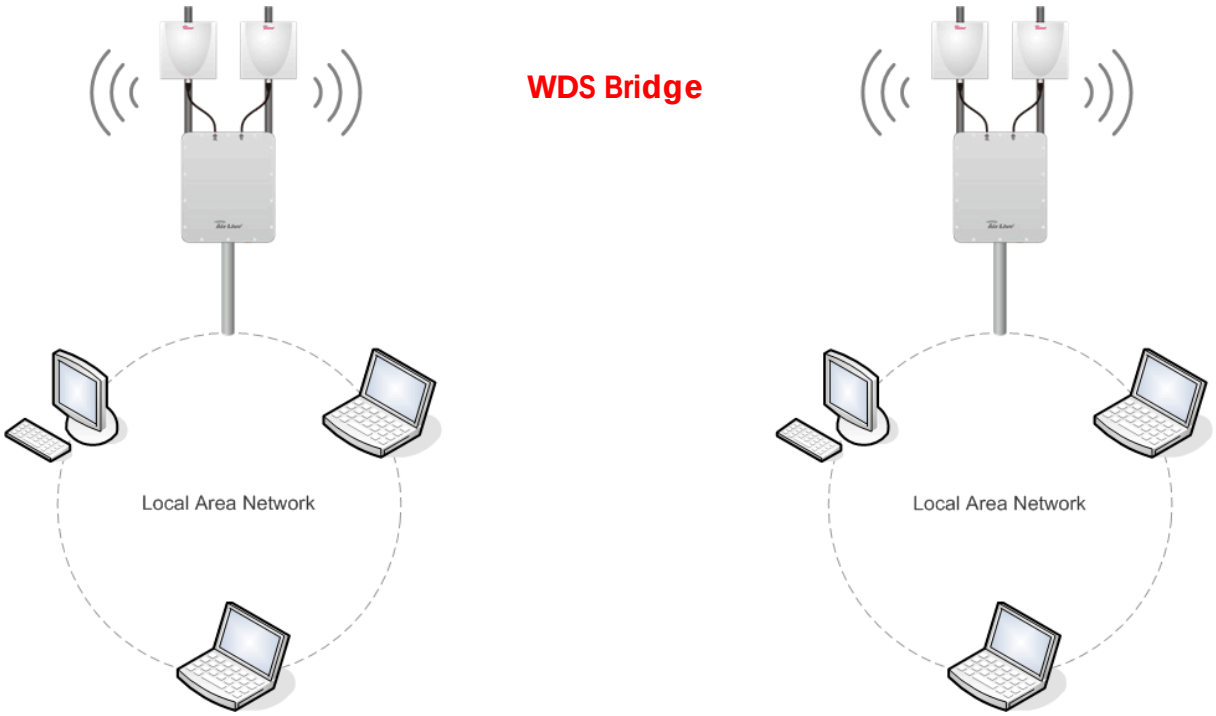
- **Network ID (SSID):** This is to change your SSID.
- **Disable SSID Broadcasting:** Enable the check box if you want to hide your SSID in the network. This prevent an un-welcomed client survey your radio.
- **Mode:** Connection modes on WH-9200AP and its wireless client. Note that the client must support the same mode as WH-9200AP to connect.
- **Channel:** 11a supports channel 36 to 64 and channel 100 to 140. 11g depends on the country, USA/Canada supports channel 1 to 11, Europe supports channel 1 to 13, Japan supports channel 1 to 13, France supports channel 10 to 13, and Span supports channel 10 to 11.
- **Enable Radio eXtended Range:** Check this box to extend the wireless coverage range, this is provided by Atheros's eXtended Range (XR) technology.
- **Enable Client Isolation (Privacy Separator):** This is to prohibit data transmission between each wireless client stations.
- **Enable 802.11d:** This is to prevent network loop applying to the spanning tree standard.

To configure the security connection, please refer to Section 3.6 Wireless Security Settings ……To configure the Advanced Settings, please refer to Section 3.7 Advanced Wireless Settings ……

To configure the access control, please refer to Section 3.8 Access Control Settings ……

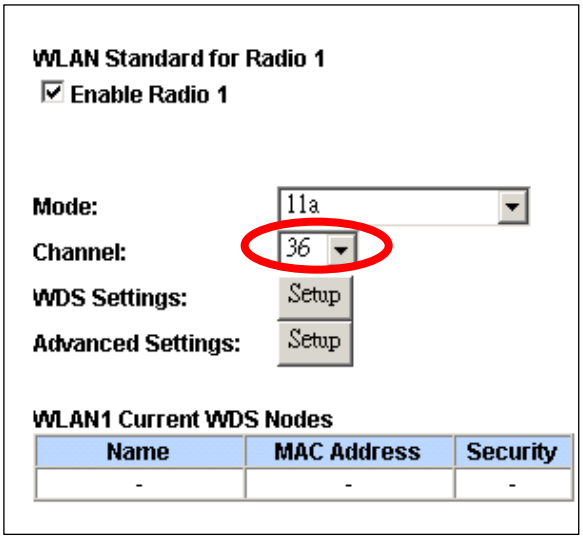
3.2 WDS Bridge Mode

In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. The bridge modes are connected by using the WDS (Wireless Distribution System) technology.



WDS Bridge mode included in these operation modes: Duplex, Dual WDS Bridge, Separate Bridge, AP + WDS Bridge, and WDS Bridge + AP.

Under WDS mode, Access Points connects to each other with MAC ID address. It's important to register the device MAC ID between each other.

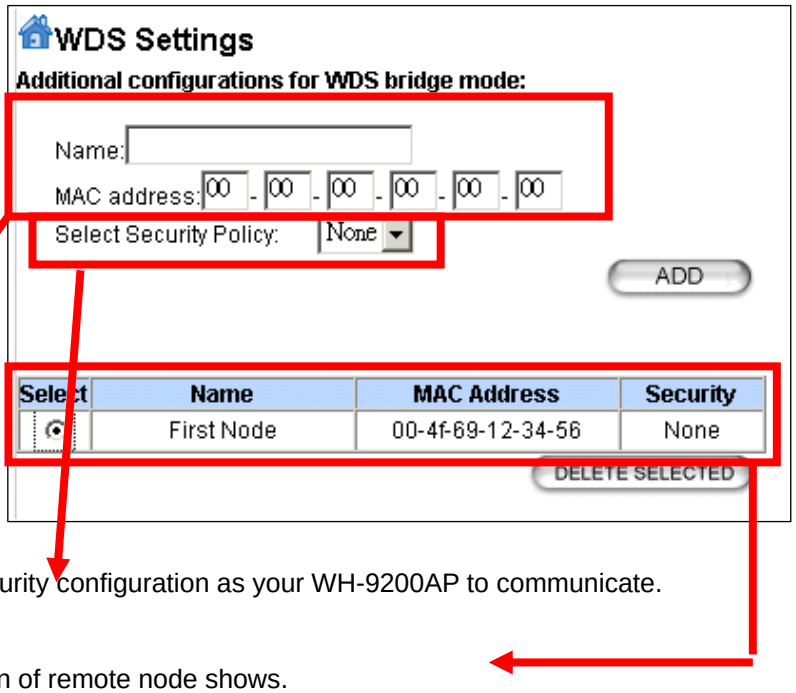


- **Enable Radio**: Use this check box to turn on or turn off the radio.
- **Mode:** Connection modes on WH-9200AP and its wireless client. Note that the client must support the same mode as WH-9200AP to connect.
- **Channel:** 11a supports channel 36 to 64 and channel 100 to 140. 11g depends on the country,

USA/Canada supports channel 1 to 11, Europe supports channel 1 to 13, Japan supports channel 1 to 13, France supports channel 10 to 13, and Span supports channel 10 to 11.

WDS Settings:

To configure WDS settings, click the WDS Settings **"Setup"** button, and the WDS Settings pop-up screen shows, please input the details of MAC ID address and desired name for remote device.

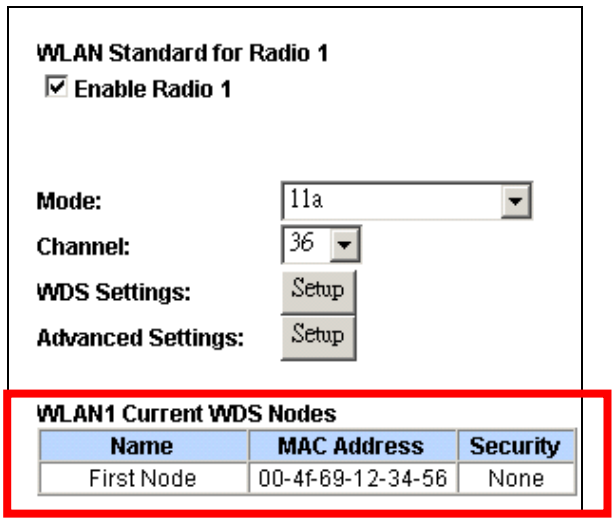


Enter the Name and MAC address of remote node which bridge to your WH-9200AP.

Only WEP security allowed in WDS mode, note that the remote node must use same security configuration as your WH-9200AP to communicate.

Click **"ADD"** button, the configured information of remote node shows.

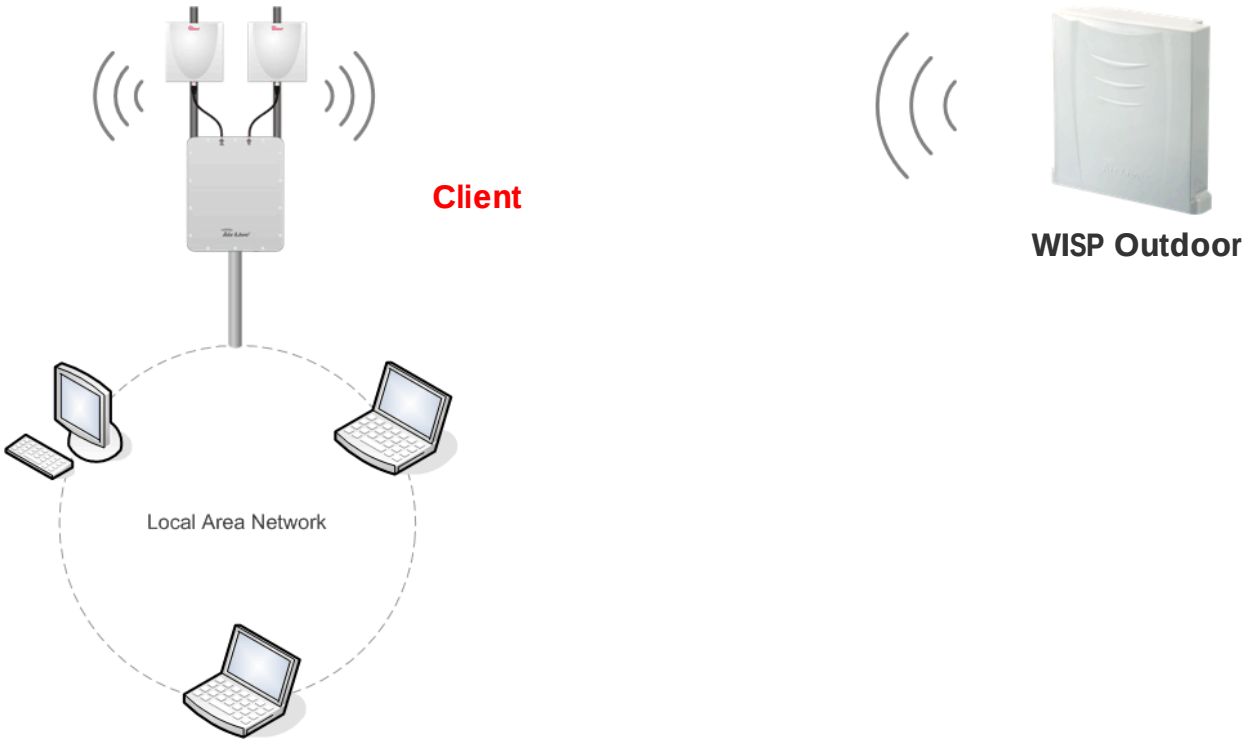
And the information shows in main configuration page as below:



To configure the Advanced Settings, please refer to Section 3.7 Advanced Wireless Settings ……

3.3 Client Mode

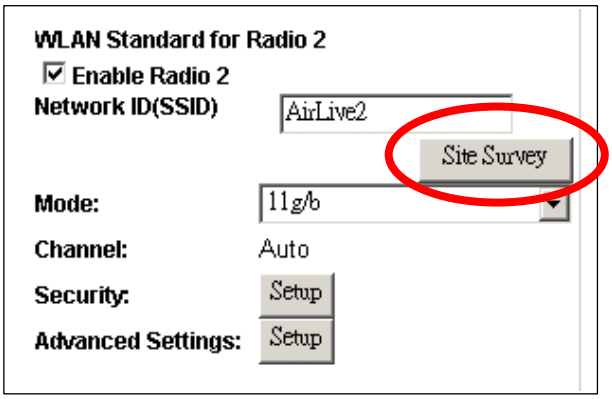
Also known as Ethernet Client. In this mode, the AP will act as a WLAN card to connect with the remote AP. Users can connect PC or local LAN to the Ethernet port of local LAN to the Ethernet port of the client mode AP. This mode is mostly used as a CPE device for WISP subscriber.

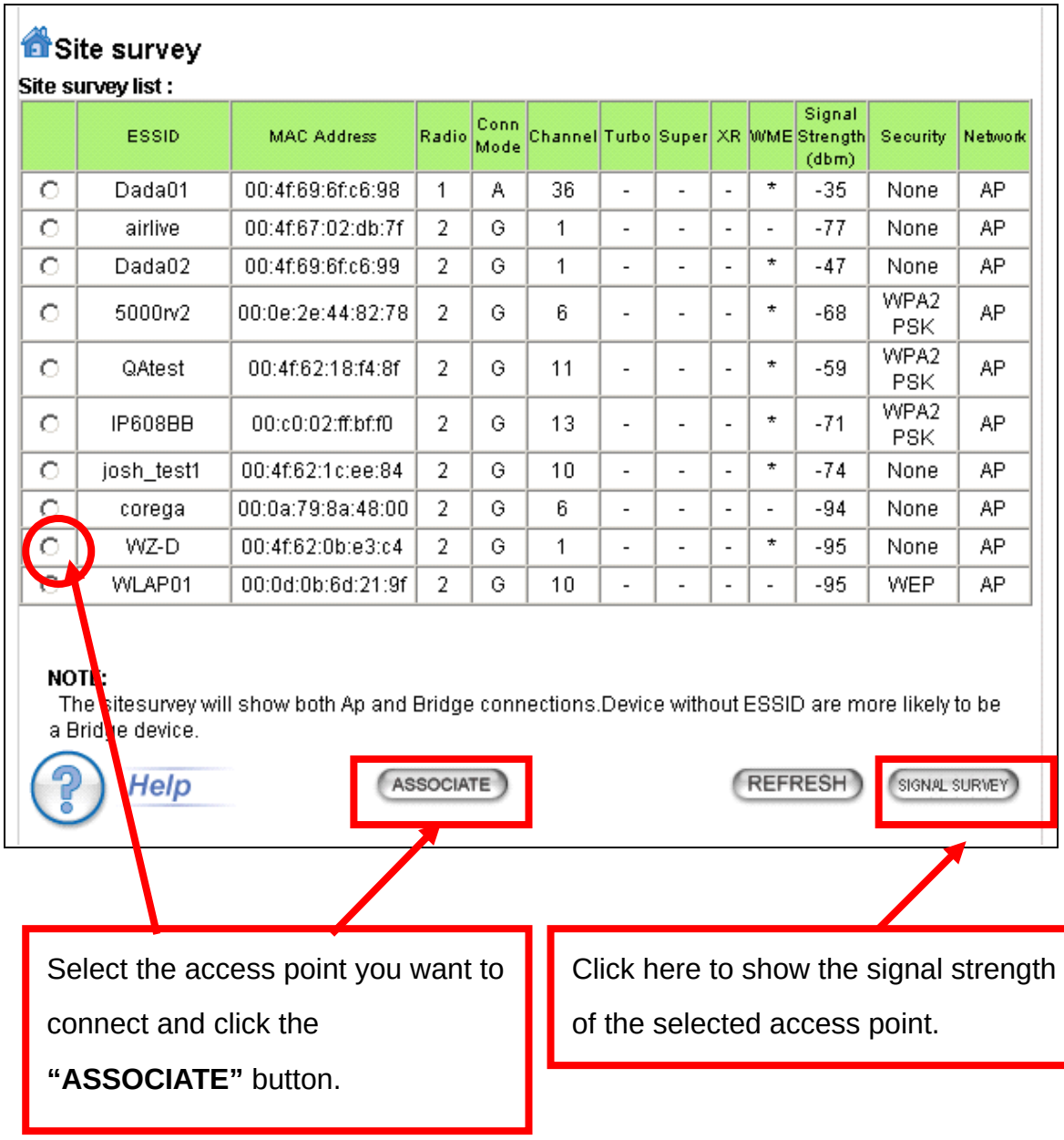


Client mode included in these operation modes: AP + Client, Client + AP, AP + WISP, and WISP + AP.

To connect to an access point, use the **"Site Survey"** button to find the Access Point.

The Site Survey pop up window then shows up and lists available access point with relative information.

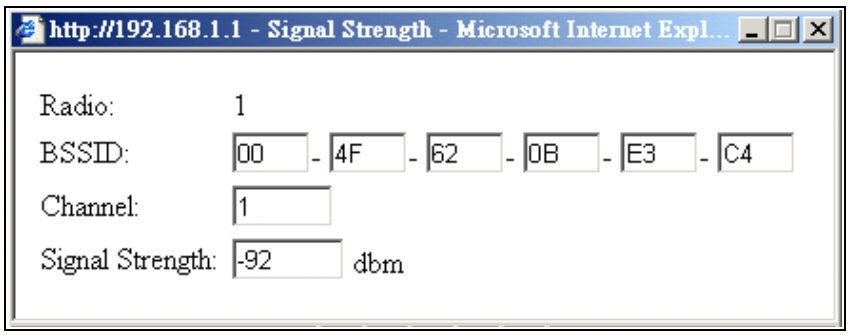



Site survey
Site survey list :
ESSID
MAC Address
Radio
Conn Mode
Channel
Turbo
Super
XR
WME
Signal Strength (dbm)
Security
Network
Dada01 00:4f:69:6f:c6:98 1 A 36 - - - * -35 None AP
airlive 00:4f:67:02:db:7f 2 G 1 - - - - -77 None AP
Dada02 00:4f:69:6f:c6:99 2 G 1 - - - * -47 None AP
5000rv2 00:0e:2e:44:82:78 2 G 6 - - - * -68 WPA2 PSK AP
QAtest 00:4f:62:18:f4:8f 2 G 11 - - - * -59 WPA2 PSK AP
IP608BB 00:c0:02:ff:bf:f0 2 G 13 - - - * -71 WPA2 PSK AP
josh_test1 00:4f:62:1c:ee:84 2 G 10 - - - * -74 None AP
corega 00:0a:79:8a:48:00 2 G 6 - - - - -94 None AP
WZ-D 00:4f:62:0b:e3:c4 2 G 1 - - - * -95 None AP
WLAP01 00:0d:0b:6d:21:9f 2 G 10 - - - - -95 WEP AP
NOTE:
The sitesurvey will show both Ap and Bridge connections.Device without ESSID are more likely to be a Bridge device.
Help
ASSOCIATE
REFRESH
SIGNAL SURVEY

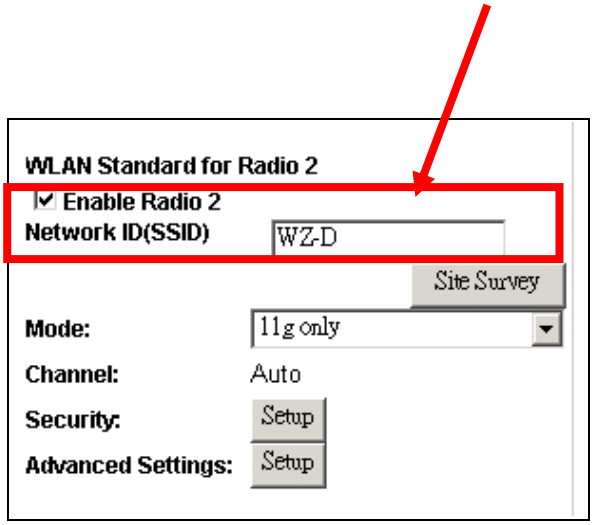
Select the access point you want to connect and click the **"ASSOCIATE"** button.

Click here to show the signal strength of the selected access point.

The Signal Survey pop up windows shows as following:



After the access point is selected, its SSID shows automatically in the Network ID (SSID) field.

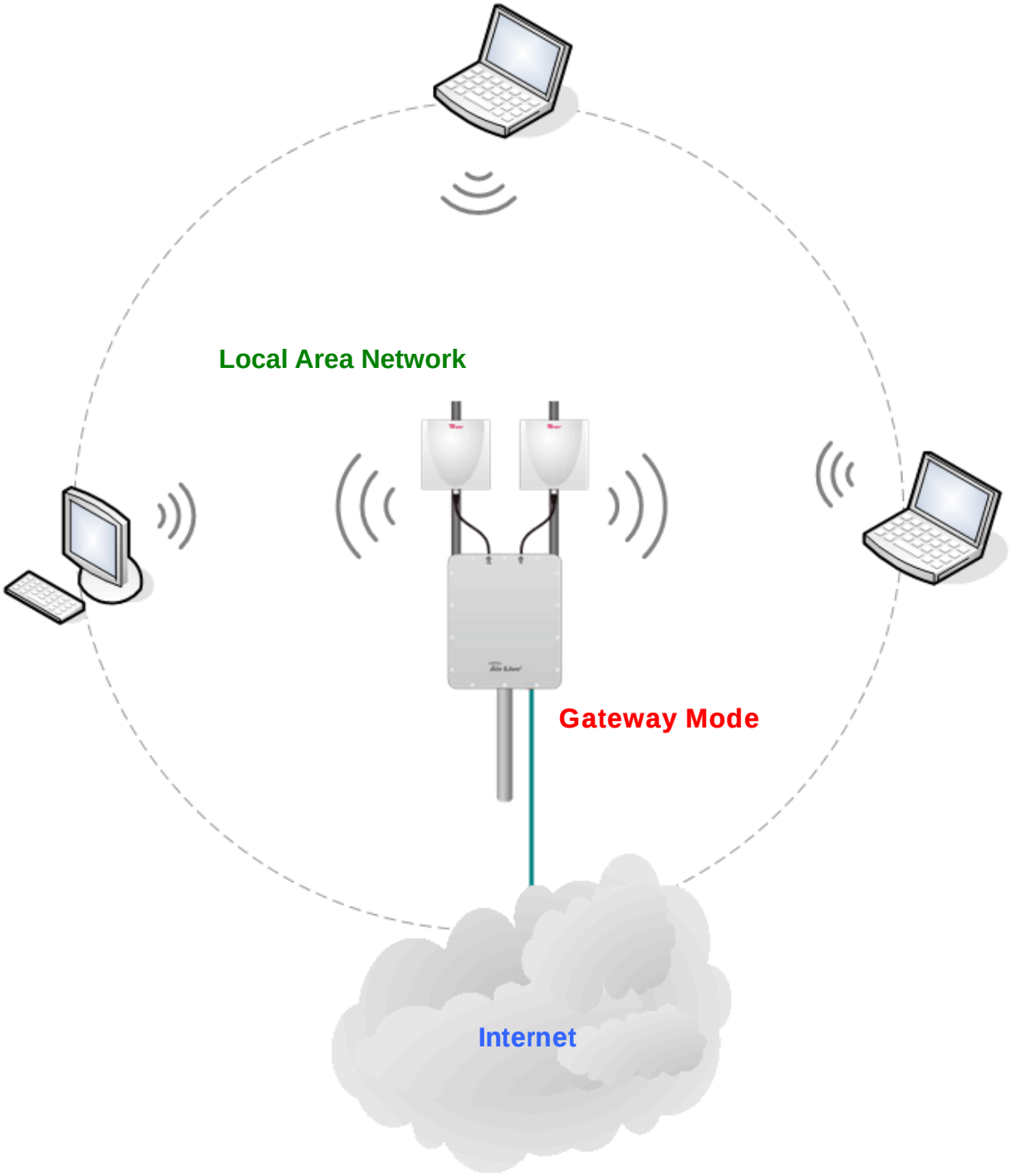


To configure the Security, please refer to Section 3.6 ……

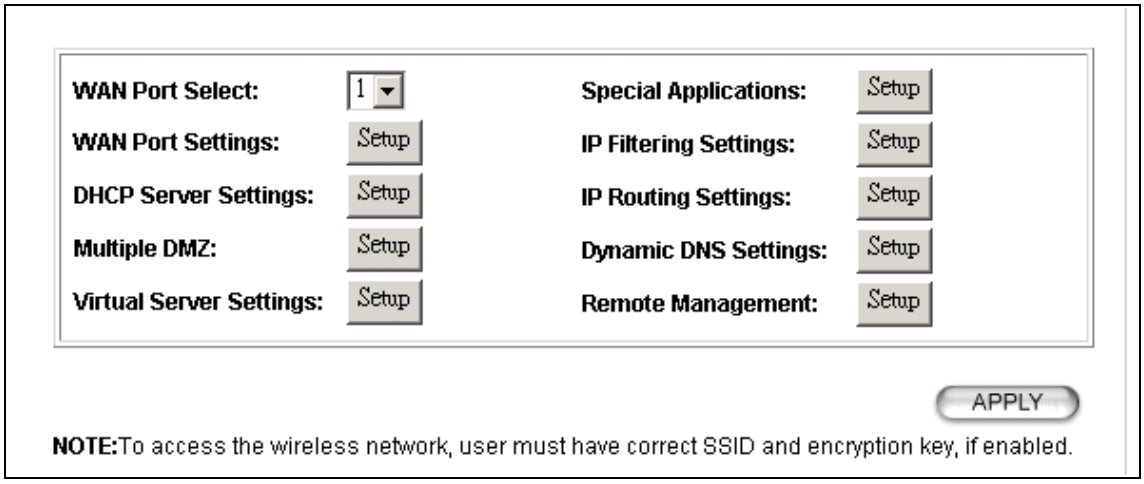
To configure the Advanced Settings, please refer to Section 3.8……

3.4 Gateway (AP Router) Mode

In Gateway mode, router functions are added between one Ethernet port and other network interfaces. Therefore, the ISP subscriber can share the ISP connection without need for extra router.



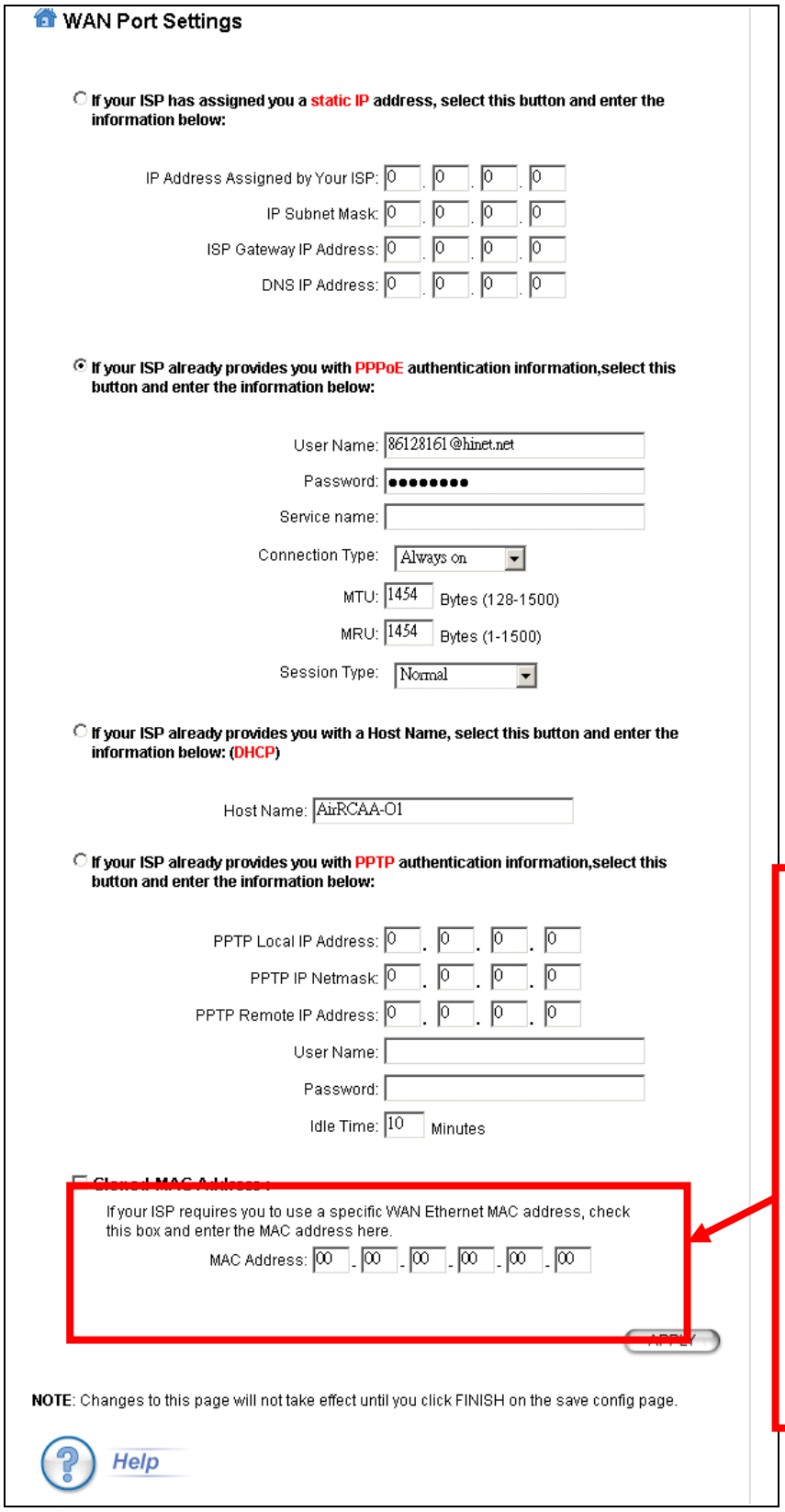
Gateway mode acts both in AP and Router which included in these operation modes: AP + Gateway and Gateway + AP.



WAN Port Select: Either the Ethernet port 1 or port 2 can be set to be the WAN port.

3.4.1 WAN Port Settings:

- Click the Setup button to configure the WAN interface.
- WH-9200AP provides 4 methods for client to access the internet. This depends on the location and the service which the ISP provides. You need to contact the ISP for detail information.


WAN Port Settings
If your ISP has assigned you a static IP address, select this button and enter the information below:
IP Address Assigned by Your ISP:
IP Subnet Mask:
ISP Gateway IP Address:
DNS IP Address:
If your ISP already provides you with PPPoE authentication information,select this button and enter the information below:
User Name: 86128161@hinet.net
Password:
Service name:
Connection Type: Always on
MTU: 1454 Bytes (128-1500)
MRU: 1454 Bytes (1-1500)
Session Type: Normal
If your ISP already provides you with a Host Name, select this button and enter the information below: (DHCP)
Host Name: AirRCAA-01
If your ISP already provides you with PPTP authentication information,select this button and enter the information below:
PPTP Local IP Address:
PPTP IP Netmask:
PPTP Remote IP Address:
User Name:
Password:
Idle Time: 10 Minutes
If your ISP requires you to use a specific WAN Ethernet MAC address, check this box and enter the MAC address here.
MAC Address:
NOTE: Changes to this page will not take effect until you click FINISH on the save config page.
Help

Clone MAC address: If your ISP allows only one MAC address for its internet access and you need more than one PC/Laptop/Server to access the internet, you can use the Clone MAC address to solve this issue.

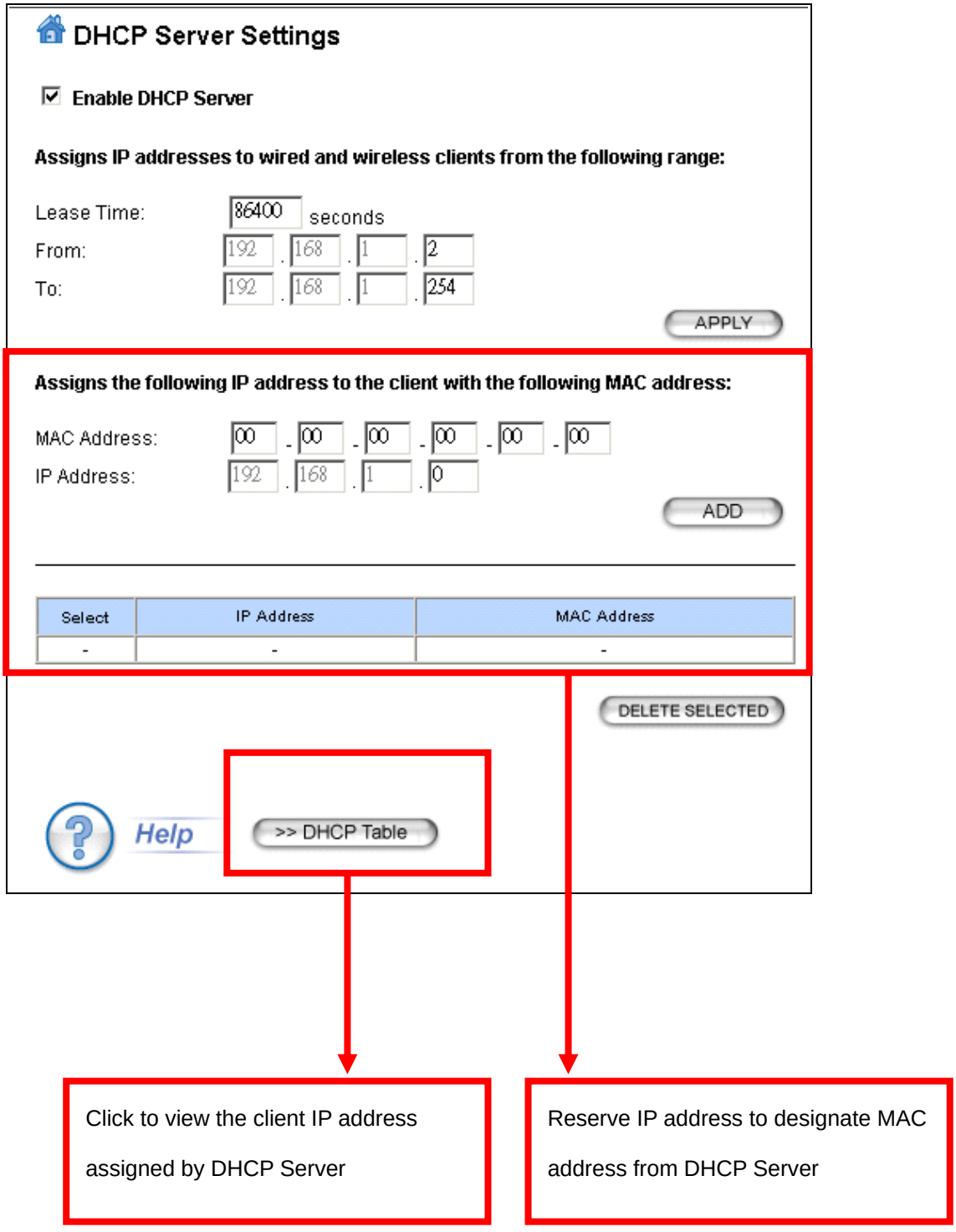
Copy either MAC of the PC/Laptop/Server which needs to access the internet in the MAC address fields.

3.4.2 DHCP Server Settings

DHCP Server Settings is to assign private IP address to the devices in your local area network (LAN).

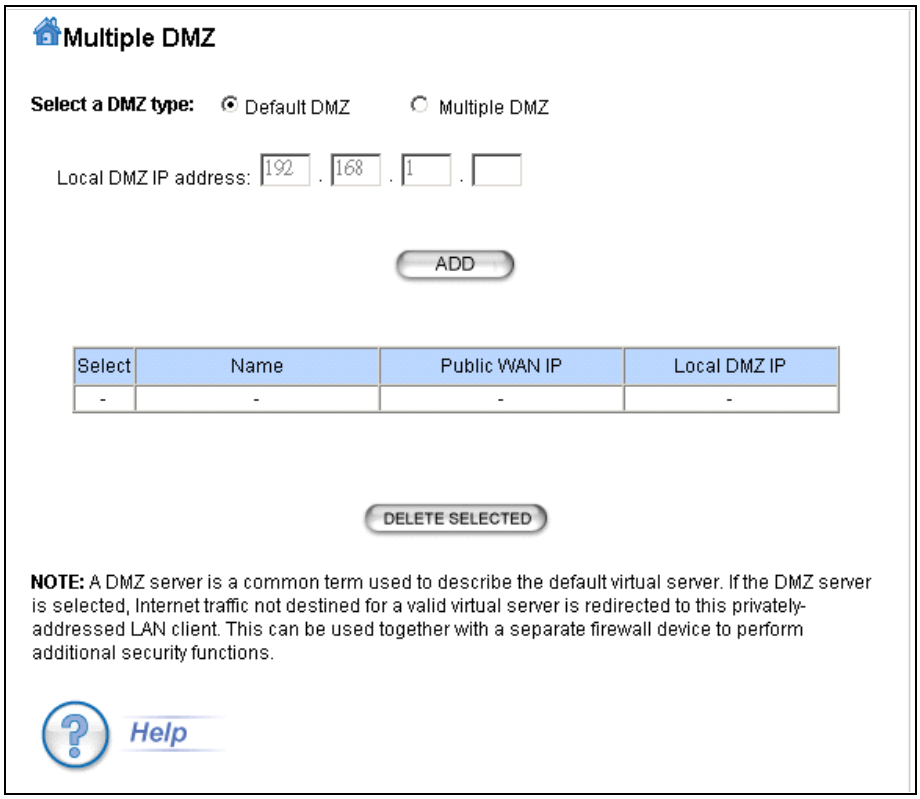
Note that WH-9200AP keep the IP address of 192.168.1.1 and act as the default gateway of the LAN.

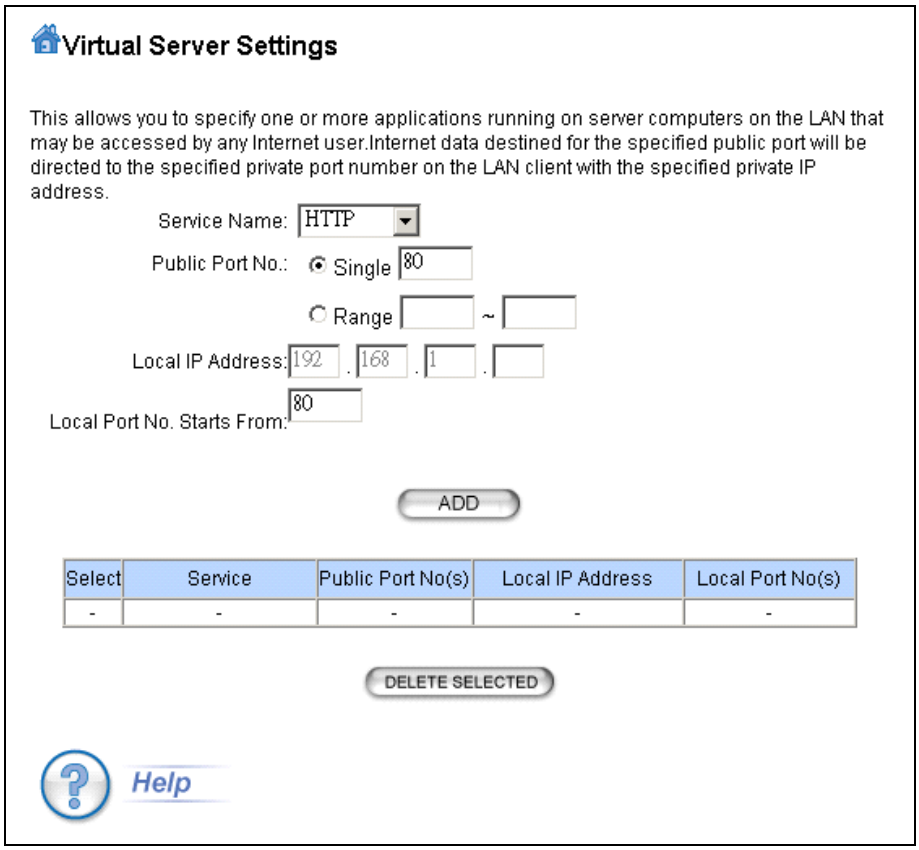
You can assign IP address to MAC address; the DHCP server will keep the IP for the MAC address.


DHCP Server Settings
Enable DHCP Server
Assigns IP addresses to wired and wireless clients from the following range:
Lease Time: 86400 seconds
From: 192 . 168 . 1 . 2
To: 192 . 168 . 1 . 254
APPLY
Assigns the following IP address to the client with the following MAC address:
MAC Address: 00 - 00 - 00 - 00 - 00 - 00
IP Address: 192 . 168 . 1 . 0
ADD
Select
IP Address
MAC Address
-
-
-
DELETE SELECTED
Help
>> DHCP Table
Click to view the client IP address assigned by DHCP Server
Reserve IP address to designate MAC address from DHCP Server

3.4.3 DMZ & Virtual Server

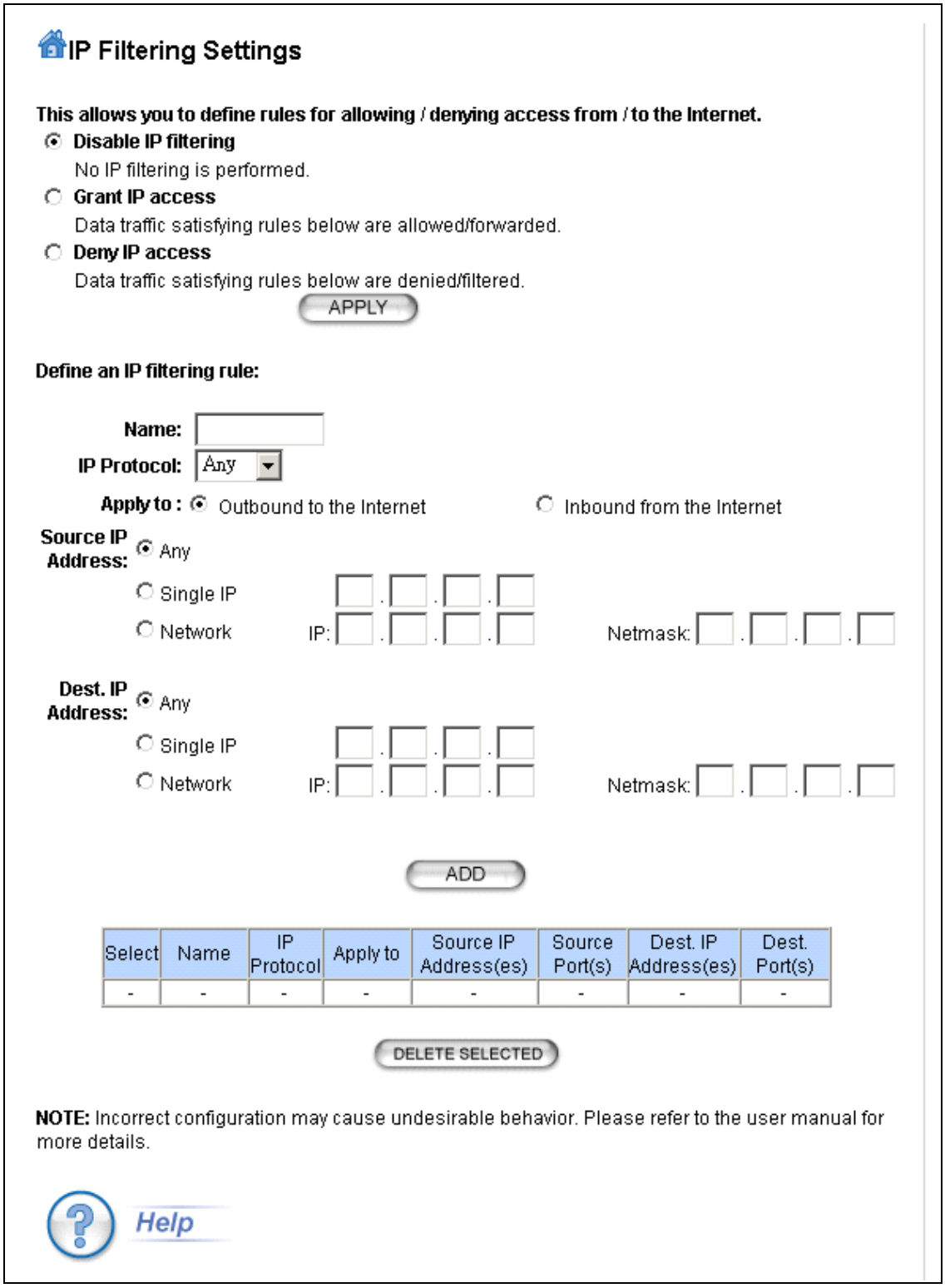
You can use DMZ and Virtual Server Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.


Multiple DMZ
Select a DMZ type:
Default DMZ
Multiple DMZ
Local DMZ IP address:
192
168
1
ADD
Select
Name
Public WAN IP
Local DMZ IP
DELETE SELECTED
NOTE: A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately-addressed LAN client. This can be used together with a separate firewall device to perform additional security functions.
Help


Virtual Server Settings
This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user.Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.
Service Name:
HTTP
Public Port No.:
Single
80
Range
Local IP Address:
192
168
1
Local Port No. Starts From:
80
ADD
Select
Service
Public Port No(s)
Local IP Address
Local Port No(s)
DELETE SELECTED
Help

3.4.4 IP Filter Settings

IP filtering is simply a mechanism that decides which types of IP datagrams will be processed normally and which will be discarded.



This allows you to define rules for allowing / denying access from / to the Internet.

Please do set both inbound/outbound in order to get complete connection. Only inbound or outbound will not allow to get response from the destination IP.

Disable IP filtering: No IP filtering is performed.

Grant IP access: Data traffic satisfying rules below are allowed/forwarded.

Deny IP access: Data traffic satisfying rules below are denied/filtered.

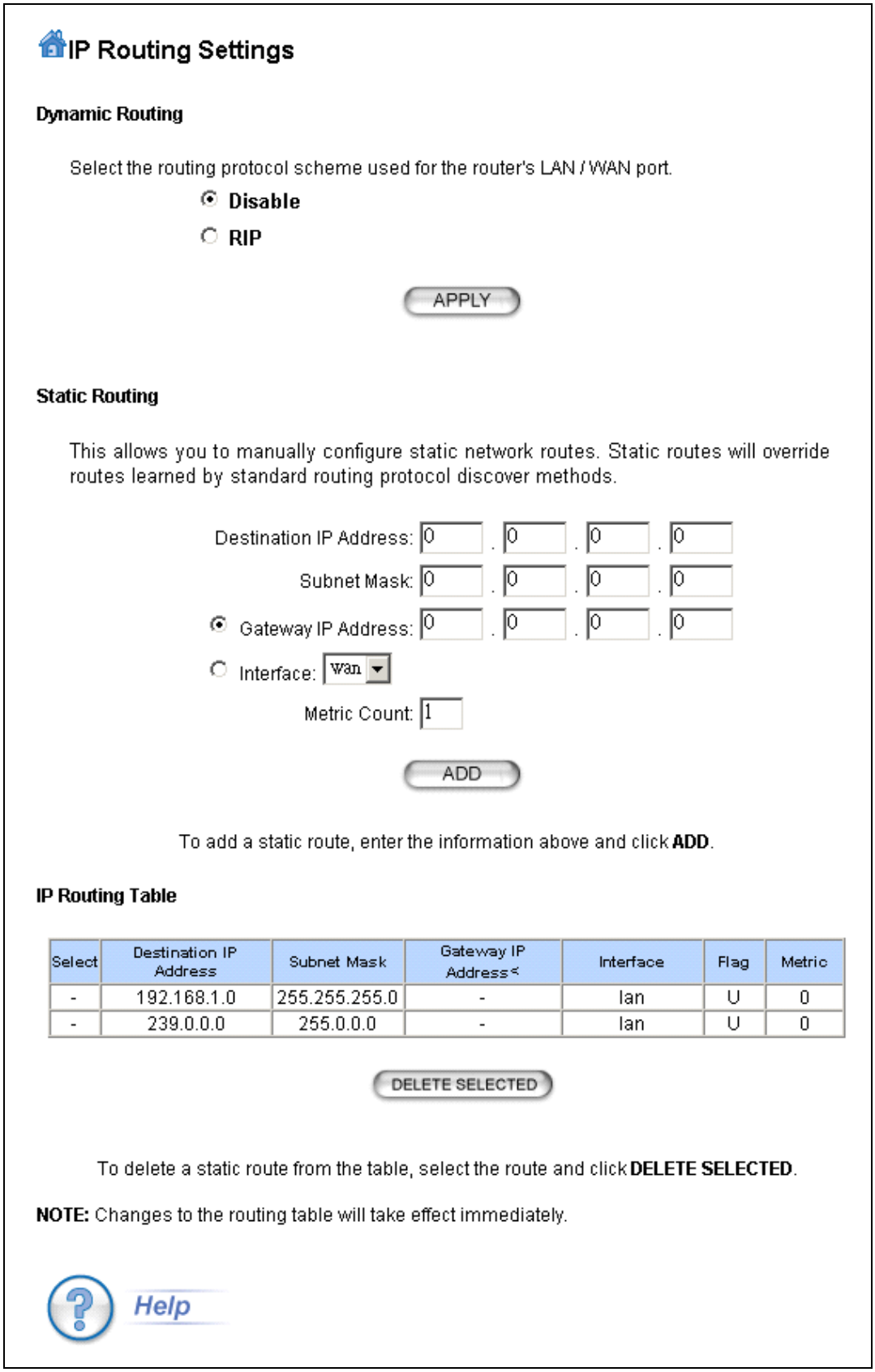
You can also define IP filtering rule, such as:

Name; IP Protocol; Apply to either Outbound to the Internet or Inbound from the Internet; Source IP Address and Dest. (Destination) IP Address.

To grant or deny IP address, select **ADD** or **Delete Selected**.

3.4.5 IP Routing Settings

The IP Routing Settings allows you to configure routing feature in the gateway, the settings is normally no need to change in gateway mode.


IP Routing Settings
Dynamic Routing
Select the routing protocol scheme used for the router's LAN / WAN port.
Disable
RIP
APPLY
Static Routing
This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.
Destination IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0
Interface: wan
Metric Count: 1
ADD
To add a static route, enter the information above and click ADD.
IP Routing Table
Select
Destination IP Address
Subnet Mask
Gateway IP Address
Interface
Flag
Metric
- 192.168.1.0 255.255.255.0 - lan U 0
- 239.0.0.0 255.0.0.0 - lan U 0
DELETE SELECTED
To delete a static route from the table, select the route and click DELETE SELECTED.
NOTE: Changes to the routing table will take effect immediately.
Help

Dynamic Routing:

Select the routing protocol scheme used for the router's LAN / WAN port.

Static Routing:

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

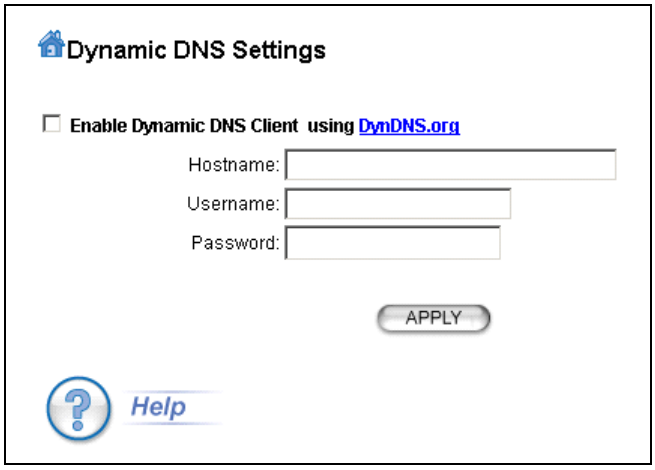
IP Routing Table:

To delete a static route from the table, select the route and click DELETE SELECTED.

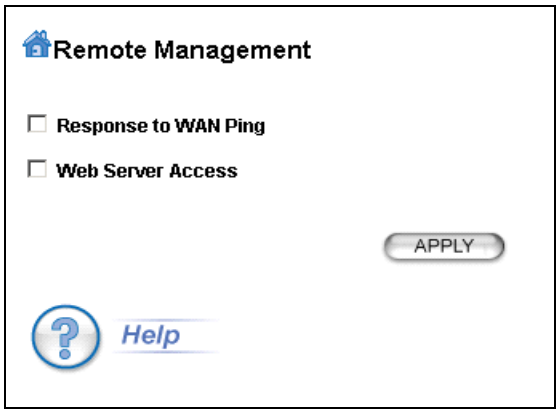
Note: Changes to the routing table will take effect immediately.

3.4.6 Dynamic DNS (DDNS) Settings

Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. WH-9200AP provide Dynamic DNS client using DynDNS, please visit http://www.dyndns.org for detail.

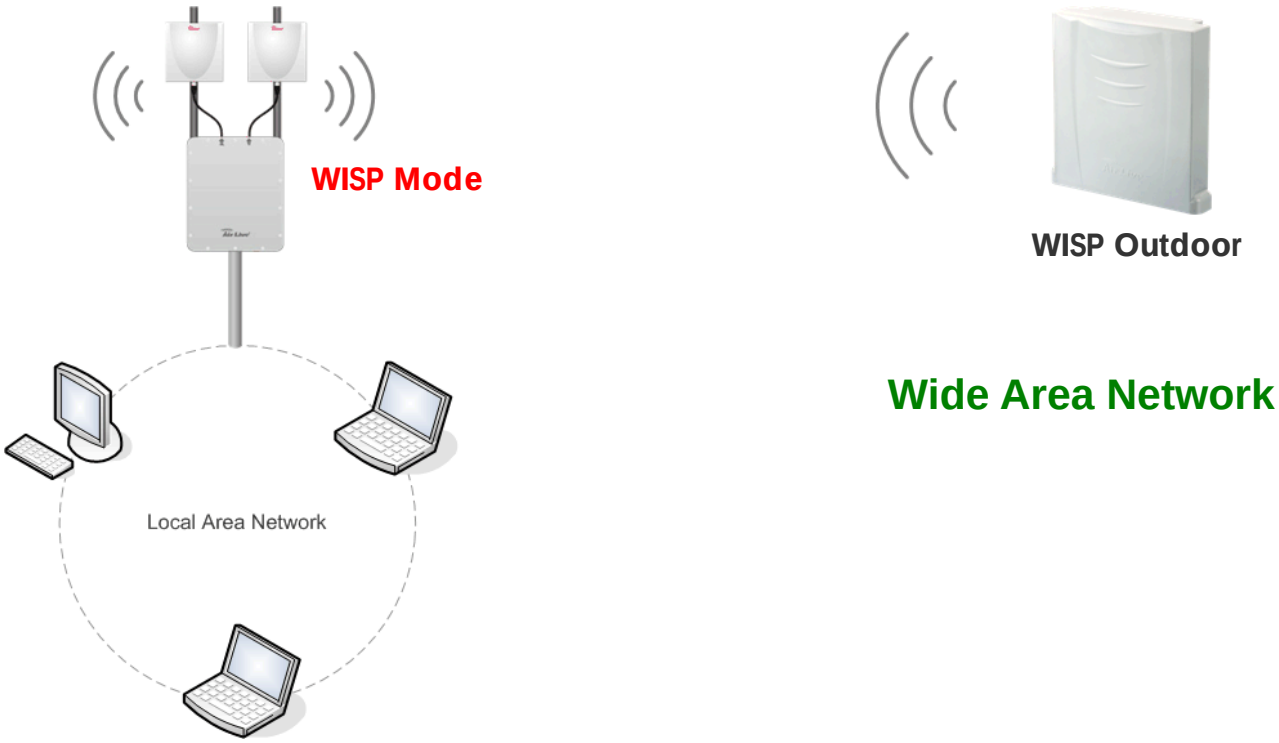


The Remote Management setting allows you to enable web server access from internet, note that this needs to configure a virtual server for your WH-9200AP. You can enable to the **"Response to WAN Ping"** to allow remotely ping your WH-9200AP.



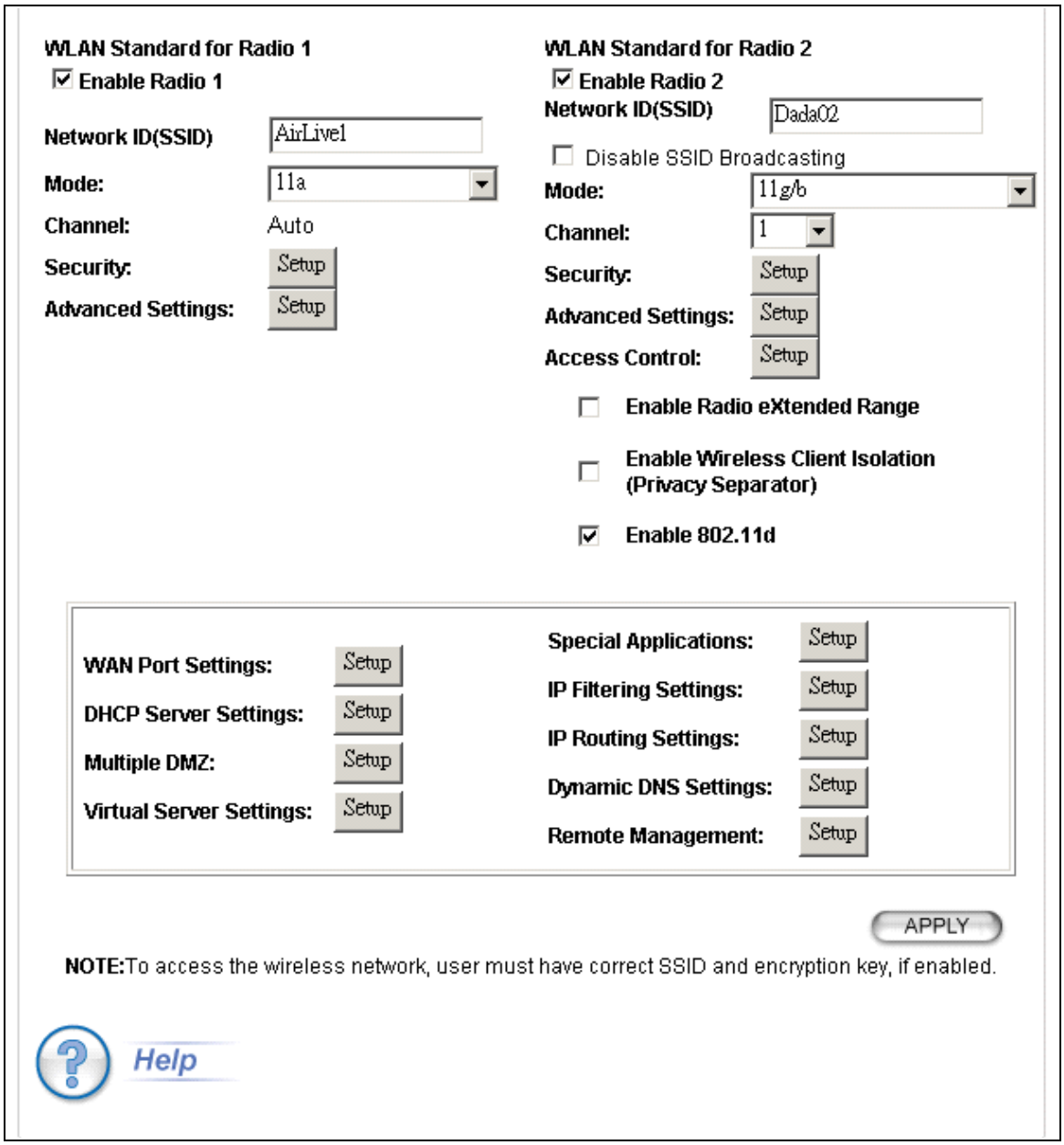
3.5 WISP Mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WISP subscriber can share the WISP connection without need for extra router.



WISP mode acts both in AP and Router which included in these operation modes: AP + WISP and WISP + AP

In WISP + AP mode, the Radio 1 is actually a wireless client of the WISP wireless node and also the gateway of the local area network.



Please refer to **Section 3.4** for gateway settings.

To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

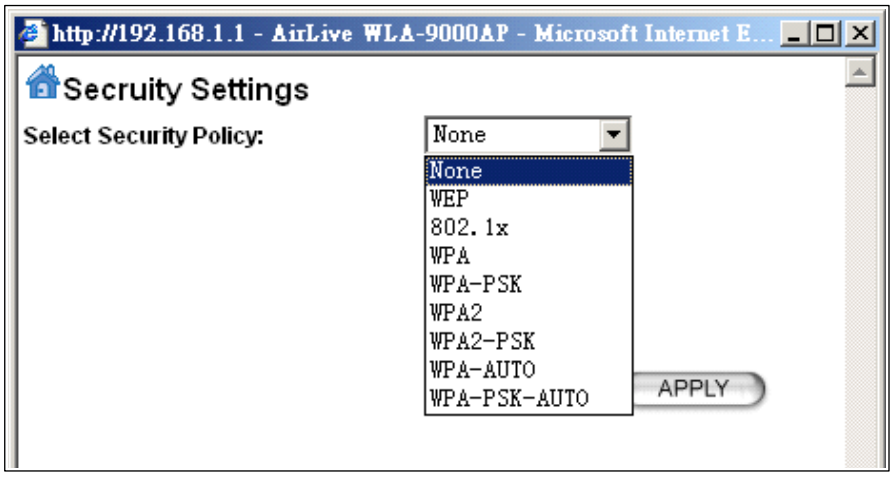
To configure the WDS mode, Please refer to Section 3.3 Client Mode ……

To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

3.6 Wireless Security

The wireless security is to configure a secure connection between two wireless devices.

WH-9200AP provides WEP, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-AUTO and WPA-PSK-AUTO security policy.



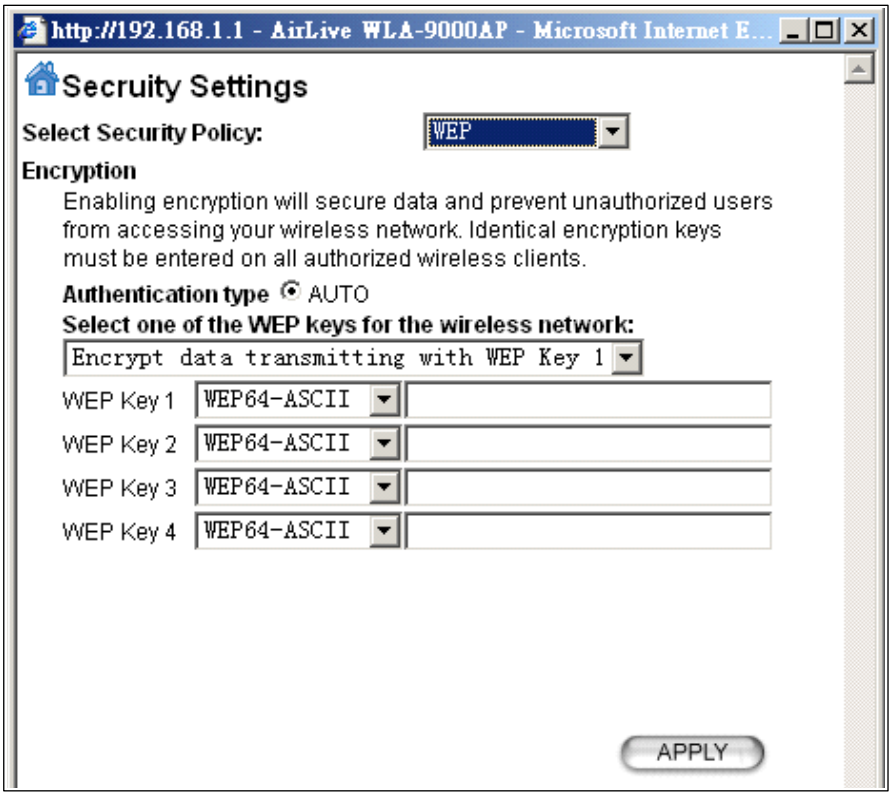
WEP

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 3 types of key: 64 (WEP64), 128 (WEP128), and 152 (WEP152) bits. You can configure up to 4 keys using either ASCII or Hexadecimal format.

Key Settings: The length of a WEP64 key must be equal to 5 bytes, a WEP128 key is 13 bytes, and a WEP152 key is 16 bytes.

Key Index: You have to specify which of the four keys will be active.

Once you enable the WEP function, please make sure that both the WH-9200AP and the wireless client stations use the same key.


http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WEP
Encryption
Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.
Authentication type AUTO
Select one of the WEP keys for the wireless network:
Encrypt data transmitting with WEP Key 1
WEP Key 1 WEP64-ASCII
WEP Key 2 WEP64-ASCII
WEP Key 3 WEP64-ASCII
WEP Key 4 WEP64-ASCII
APPLY

Some wireless client cards only allow Hexadecimal digits for WEP keys.

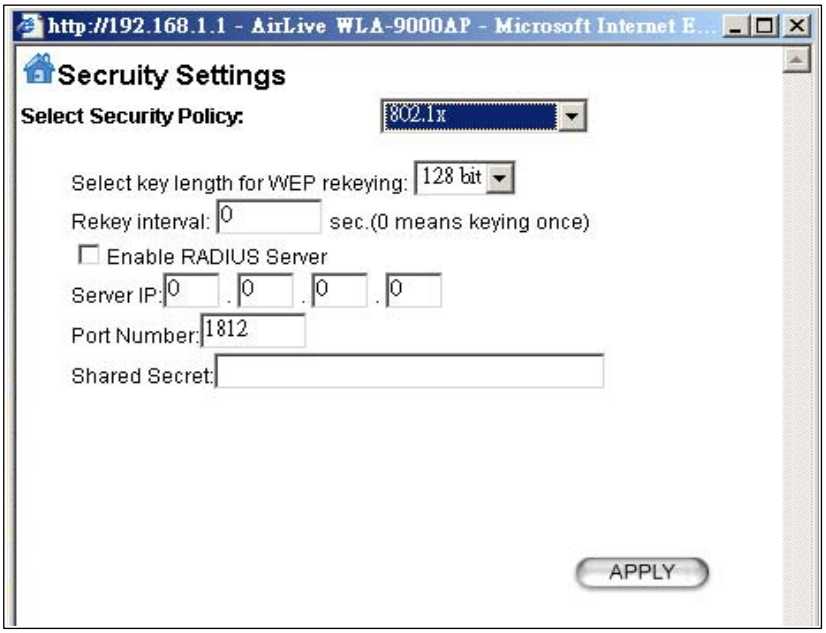
Please note that when configuring WEP keys, a WEP128 ASCII key looks like

"**This is a key**"(13 characters), while a WEP128 Hex key looks like "**54686973206973206120b6579**"(26 HEX)

(hexadecimal notation are 0-9 and A-F).

802.1X

802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP key (128 bit) to have data encryption. Here you do not have to enter the WEP key manually because it will be generated automatically and dynamically.



Rekey interval is time period that the system will change the key periodically. The shorter the interval is, the better the security is.

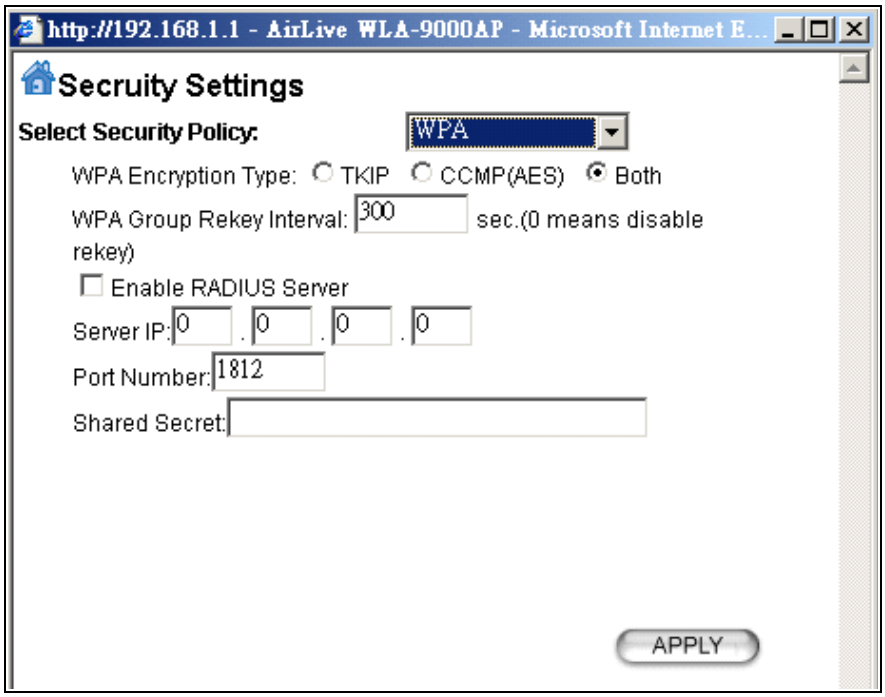
Server IP and Shared Secret: If you have connect AP to a RADIUS server behind, key in the Server IP and share secret, it will redirect incoming connection request first to this RADIUS for Authentication. In general you don't have to change Port Number, which is 1812 by default and used by most RADIUS server.

After you have finished the configuration wizard, you have to configure the RADIUS Settings in Advanced Settings in order to make the 802.1x function work.

Share secret is the key for AP to communicate with RADIUS server, check with your Authentication provider for more details.

WPA

Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

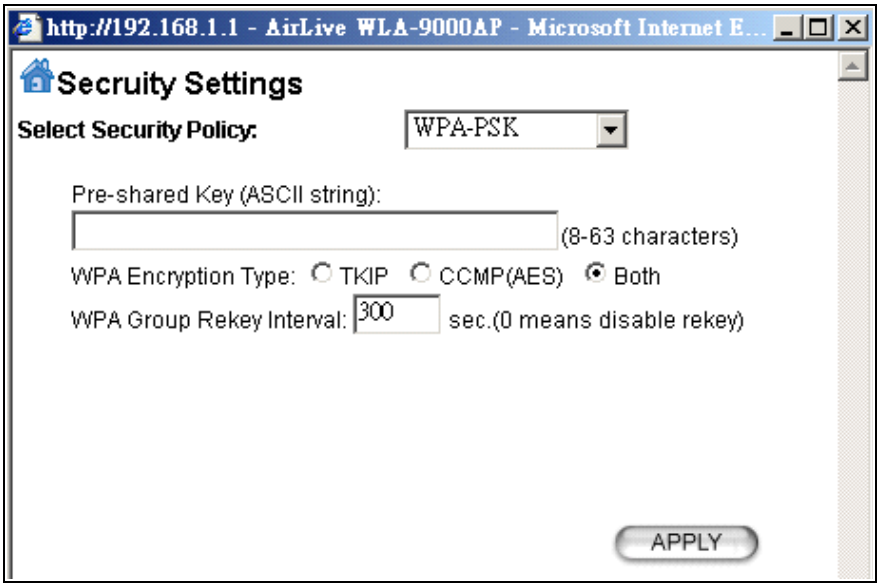

http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA
WPA Encryption Type: TKIP CCMP(AES) Both
WPA Group Rekey Interval: 300 sec.(0 means disable rekey)
Enable RADIUS Server
Server IP: 0 . 0 . 0 . 0
Port Number: 1812
Shared Secret:
APPLY

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.


http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA-PSK
Pre-shared Key (ASCII string):
(8-63 characters)
WPA Encryption Type: TKIP CCMP(AES) Both
WPA Group Rekey Interval: 300 sec.(0 means disable rekey)
APPLY

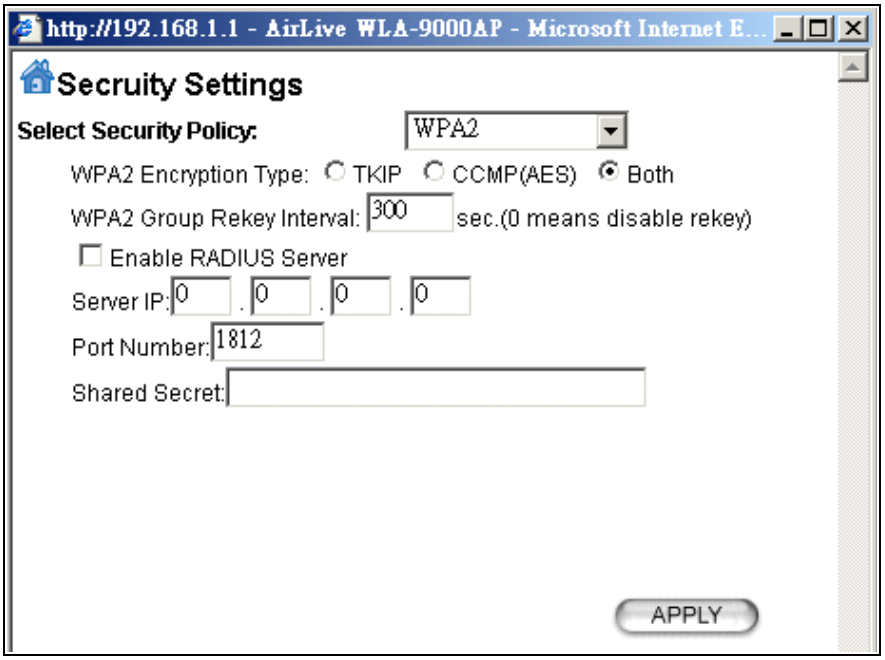
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2

WPA2 stands for Wi-Fi Protected Access 2. It provides stronger data protection and network access control then WPA. Only authorized users can access the wireless networks.

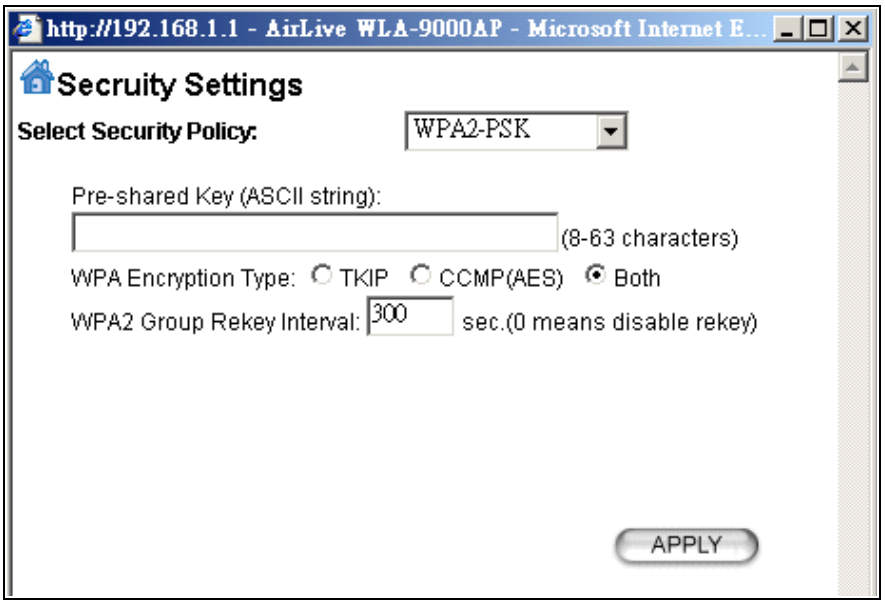

http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA2
WPA2 Encryption Type: TKIP CCMP(AES) Both
WPA2 Group Rekey Interval: 300 sec.(0 means disable rekey)
Enable RADIUS Server
Server IP: 0 . 0 . 0 . 0
Port Number: 1812
Shared Secret:
APPLY

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2-PSK

Enter the Pre-shared Key to initiate WPA2 security. All devices try to access the network should have the matching encryption key.

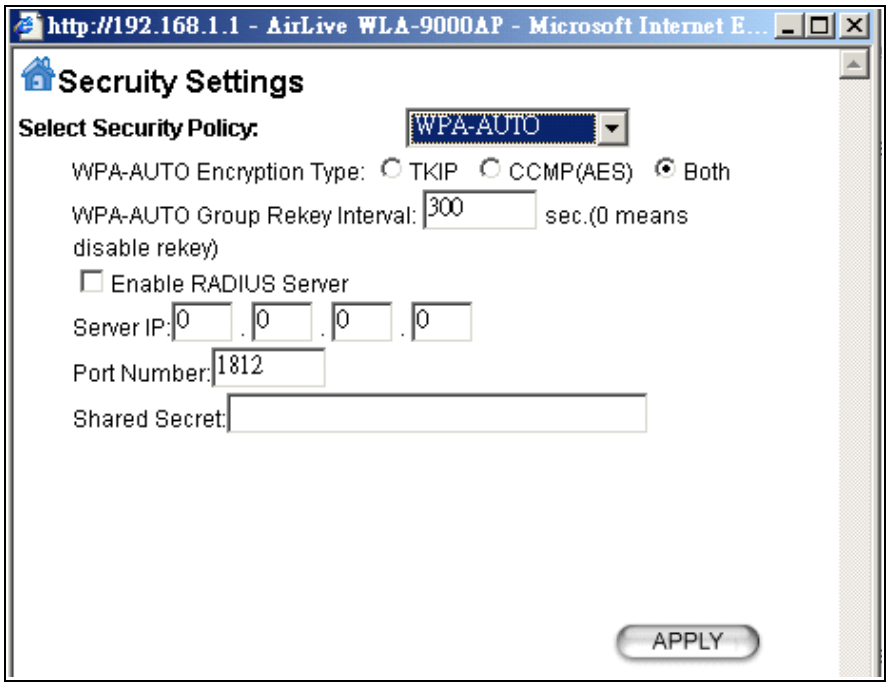

http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA2-PSK
Pre-shared Key (ASCII string):
(8-63 characters)
WPA Encryption Type: TKIP CCMP(AES) Both
WPA2 Group Rekey Interval: 300 sec.(0 means disable rekey)
APPLY

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-AUTO

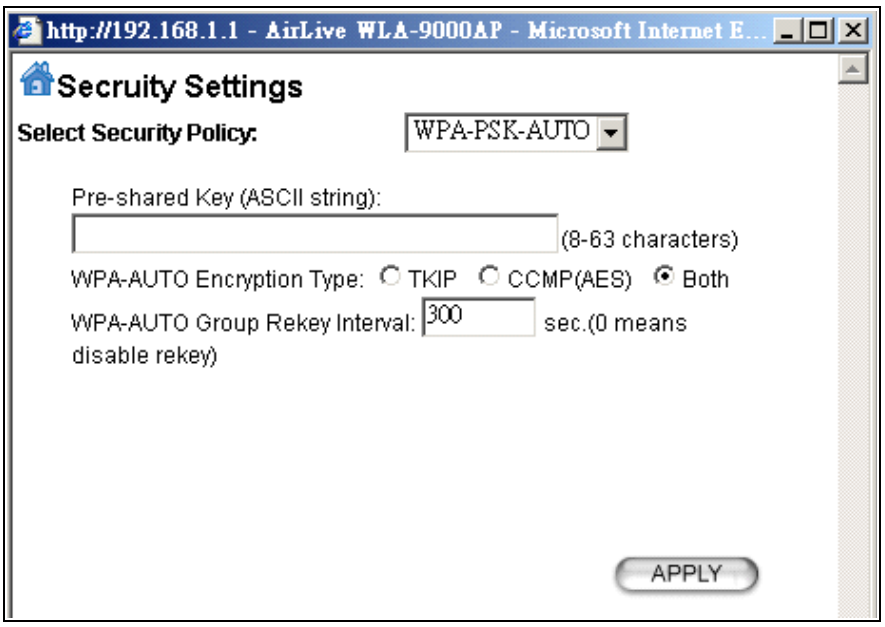

http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA-AUTO
WPA-AUTO Encryption Type: TKIP CCMP(AES) Both
WPA-AUTO Group Rekey Interval: 300 sec.(0 means disable rekey)
Enable RADIUS Server
Server IP: 0 . 0 . 0 . 0
Port Number: 1812
Shared Secret:
APPLY

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK-AUTO

WPA-PSK-AUTO tries to authenticate wireless clients using WPA-PSK or WPA2-PSK.


http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet E...
Secruity Settings
Select Security Policy:
WPA-PSK-AUTO
Pre-shared Key (ASCII string):
(8-63 characters)
WPA-AUTO Encryption Type: TKIP CCMP(AES) Both
WPA-AUTO Group Rekey Interval: 300 sec.(0 means disable rekey)
APPLY

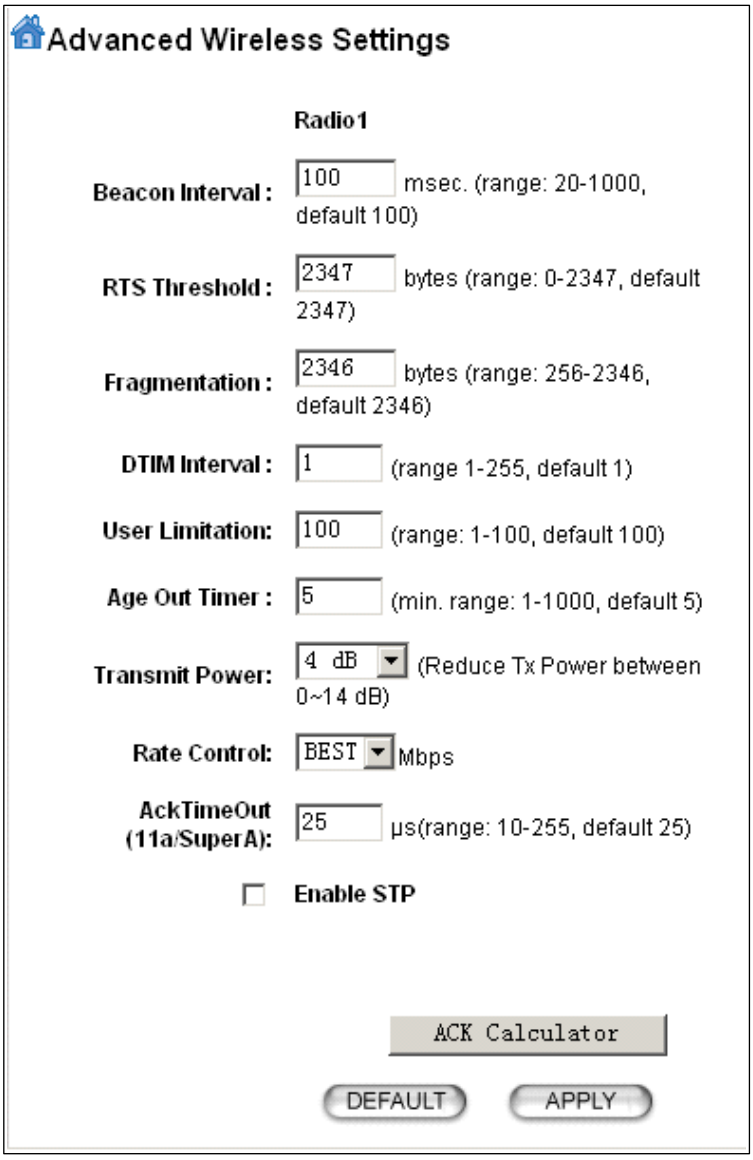
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

3.7 Advanced Wireless Settings

When click on Advanced Setup button under client mode, a pop-up window appears and show parameter as follow:



Beacon Interval: The WH-9200AP broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds.

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of 2347. It is recommended that this value does not deviate from the default too much.

Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The WH-9200AP buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs.

User Limitation: The range of user limitation is from 1 to 100.

Age Out Timer: Set the age out time. The default is 300 sec.

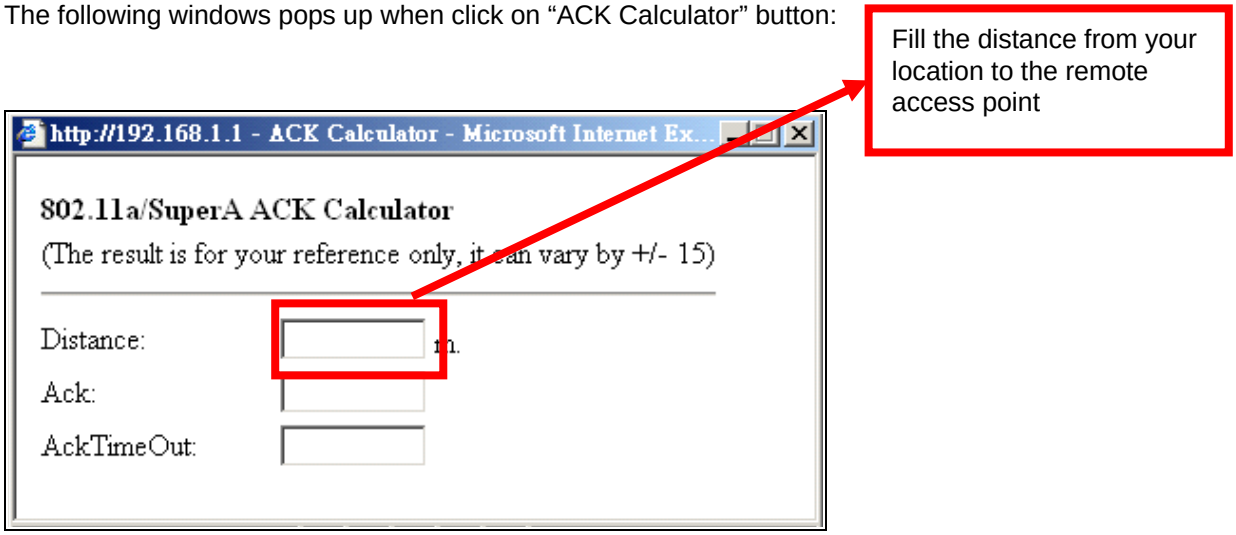
Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Rate Control: Limit the wireless data rate to the selected number.

Enable STP: Spanning Tree Protocol prevents the condition known as a bridge loop.

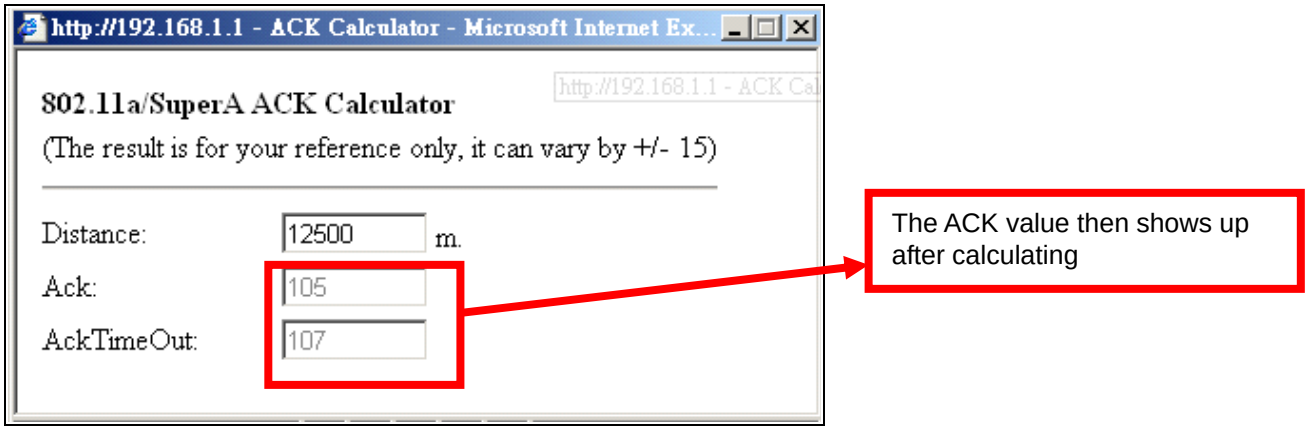
Ack TimeOut: The **"ACK time-out"** determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file.

The following windows pops up when click on “ACK Calculator” button:

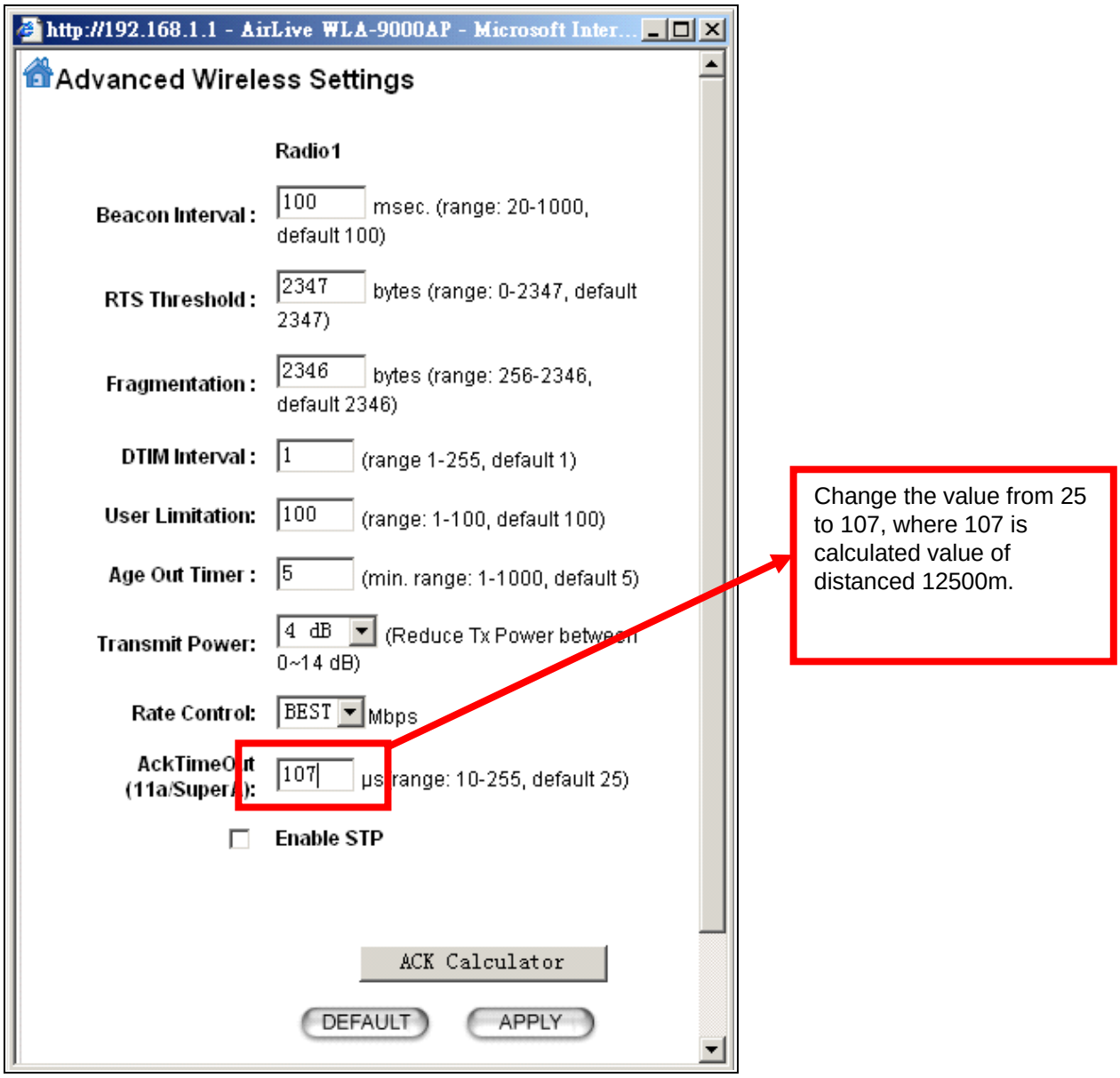

Fill the distance from your location to the remote access point
http://192.168.1.1 - ACK Calculator - Microsoft Internet Ex...
802.11a/SuperA ACK Calculator
(The result is for your reference only, it can vary by +/- 15)
Distance:
m.
Ack:
AckTimeOut:

In the field of **“Distance”**, input the distance in **“meters”**.

After input the distance value, move the cursor to any place on the pop-up window out of three fields. The calculated value will display.


http://192.168.1.1 - ACK Calculator - Microsoft Internet Ex...
802.11a/SuperA ACK Calculator
(The result is for your reference only, it can vary by +/- 15)
Distance: 12500 m.
Ack: 105
AckTimeOut: 107
The ACK value then shows up after calculating

Enter the calculated value of **"AckTimeOut"** into the appropriate **"Ack TimeOut"** field (11a or 11g) in the **"Advanced Wireless Settings"** window.


http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Inter...
Advanced Wireless Settings
Radio1
Beacon Interval: 100 msec. (range: 20-1000, default 100)
RTS Threshold: 2347 bytes (range: 0-2347, default 2347)
Fragmentation: 2346 bytes (range: 256-2346, default 2346)
DTIM Interval: 1 (range 1-255, default 1)
User Limitation: 100 (range: 1-100, default 100)
Age Out Timer: 5 (min. range: 1-1000, default 5)
Transmit Power: 4 dB (Reduce Tx Power between 0~14 dB)
Rate Control: BEST Mbps
AckTimeOut (11a/SuperA): 107 μs (range: 10-255, default 25)
Enable STP
ACK Calculator
DEFAULT
APPLY
Change the value from 25 to 107, where 107 is calculated value of distanced 12500m.

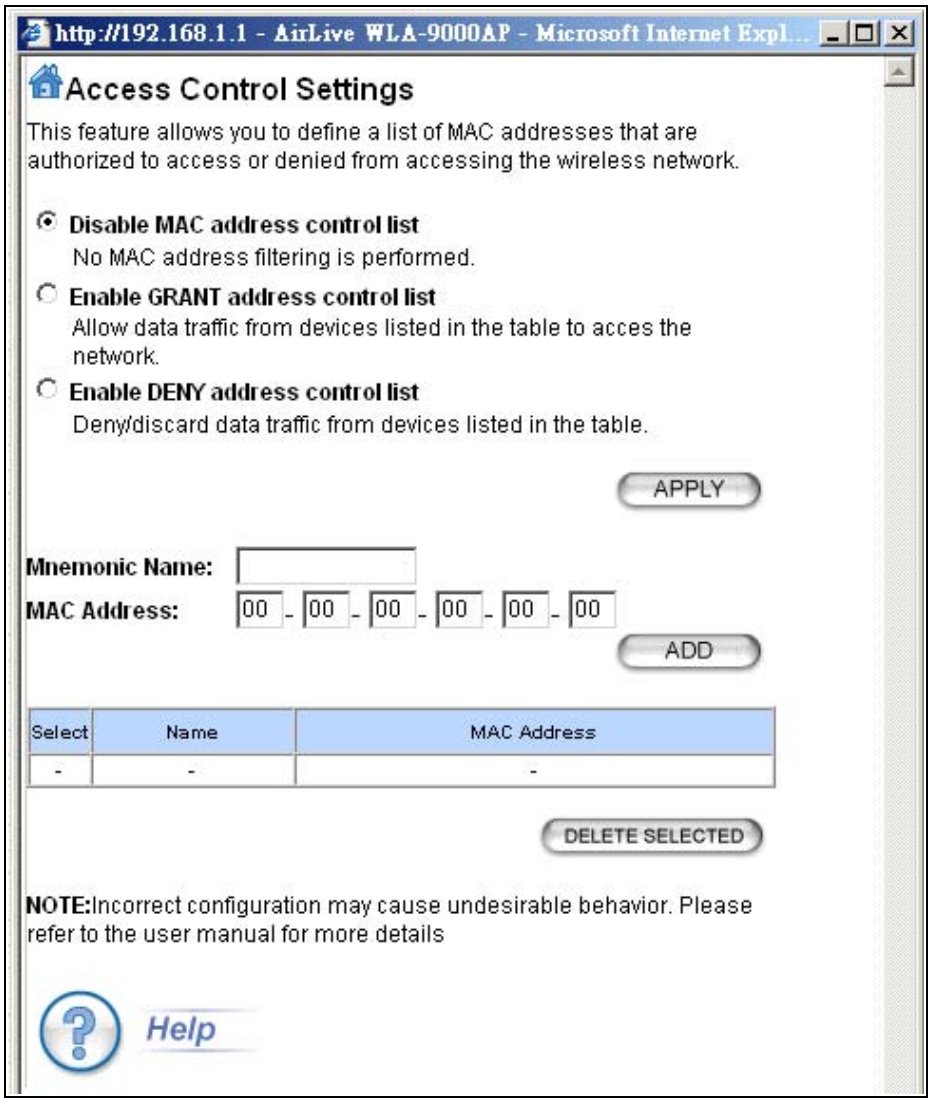
3.8 Access Control

The WH-9200AP allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. Click on the setup button of “Access Control” of selected wireless interface.

Disable MAC address control list: When selected, no MAC address filtering will be performed.

Enable GRANT address control list: When selected, data traffic from only the specified devices in the table will be allowed in the network.

Enable DENY address control list: When selected, data traffic from the devices specified in the table will be denied/discarded by the network.


http://192.168.1.1 - AirLive WLA-9000AP - Microsoft Internet Expl...
Access Control Settings
This feature allows you to define a list of MAC addresses that are authorized to access or denied from accessing the wireless network.
Disable MAC address control list
No MAC address filtering is performed.
Enable GRANT address control list
Allow data traffic from devices listed in the table to acces the network.
Enable DENY address control list
Deny/discard data traffic from devices listed in the table.
APPLY
Mnemonic Name:
MAC Address:
00 - 00 - 00 - 00 - 00 - 00
ADD
Select
Name
MAC Address
DELETE SELECTED
NOTE:Incorrect configuration may cause undesirable behavior. Please refer to the user manual for more details
Help

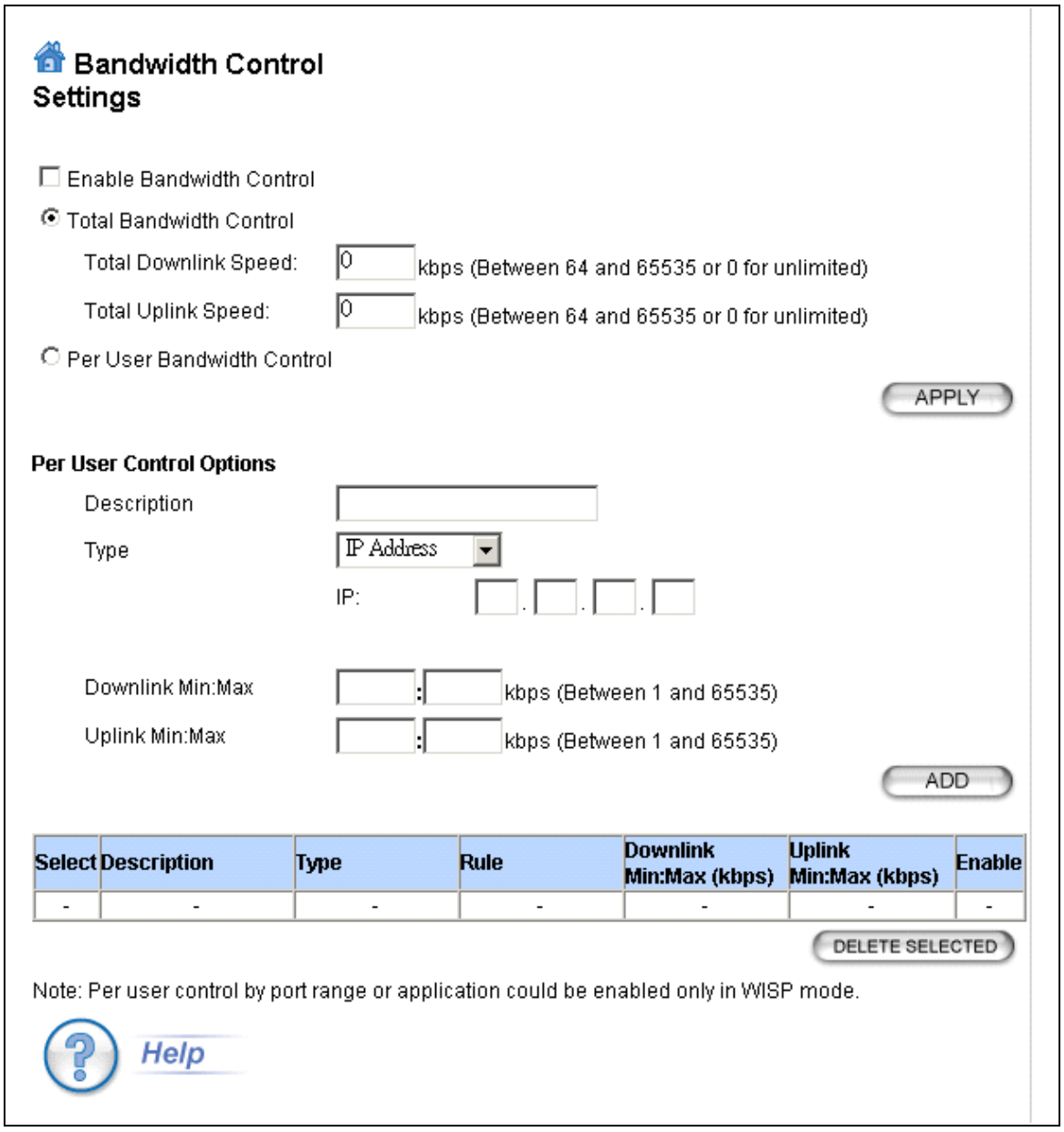
To add a MAC address into the table, enter a Mnemonic Name and the MAC Address, and then click ADD. The table lists all configured MAC Filter entries.

To delete entries, check the corresponding Select boxes and then press DELETE SELECTED.

3.9 Bandwidth Control

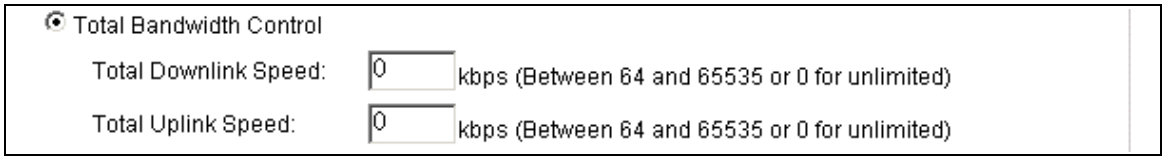
Bandwidth Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance firmware can control the bandwidth by Interface or IP/MAC.

There are 2 types of Traffic Control it offers: Total bandwidth control and Per-use bandwidth control.



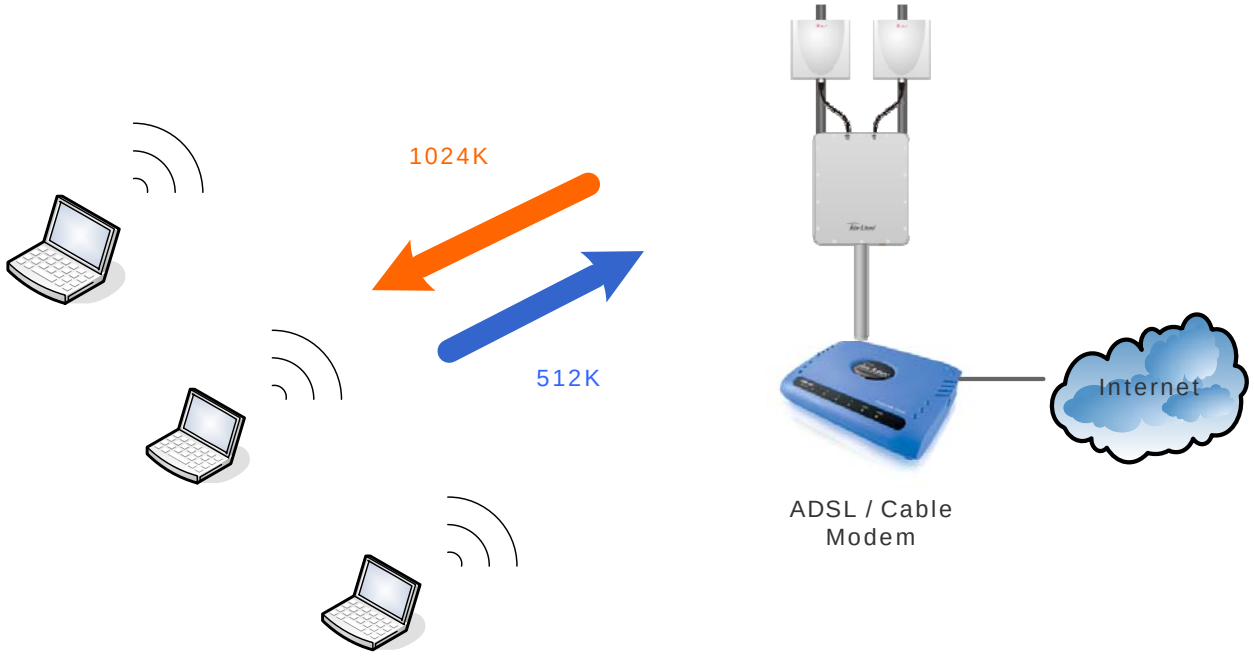
3.9.1 Total Bandwidth Control

The total bandwidth controls the data rate at either Wired or Wireless interface.


Total Bandwidth Control
Total Downlink Speed:
0
kbps (Between 64 and 65535 or 0 for unlimited)
Total Uplink Speed:
0
kbps (Between 64 and 65535 or 0 for unlimited)

The following example limit the download bandwidth to **1024kbps** and uplink to **512kbps**

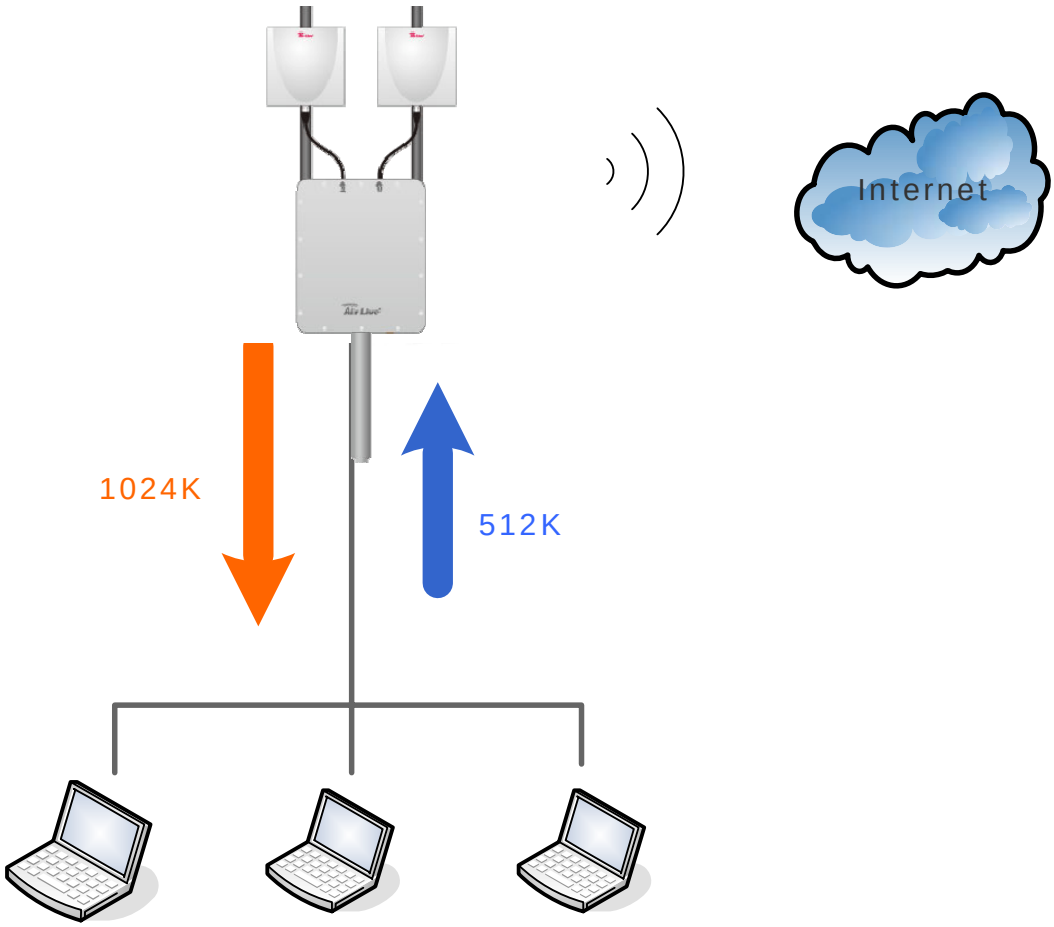
Example1: 3 wireless clients share downlink and uplink bandwidth.



In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

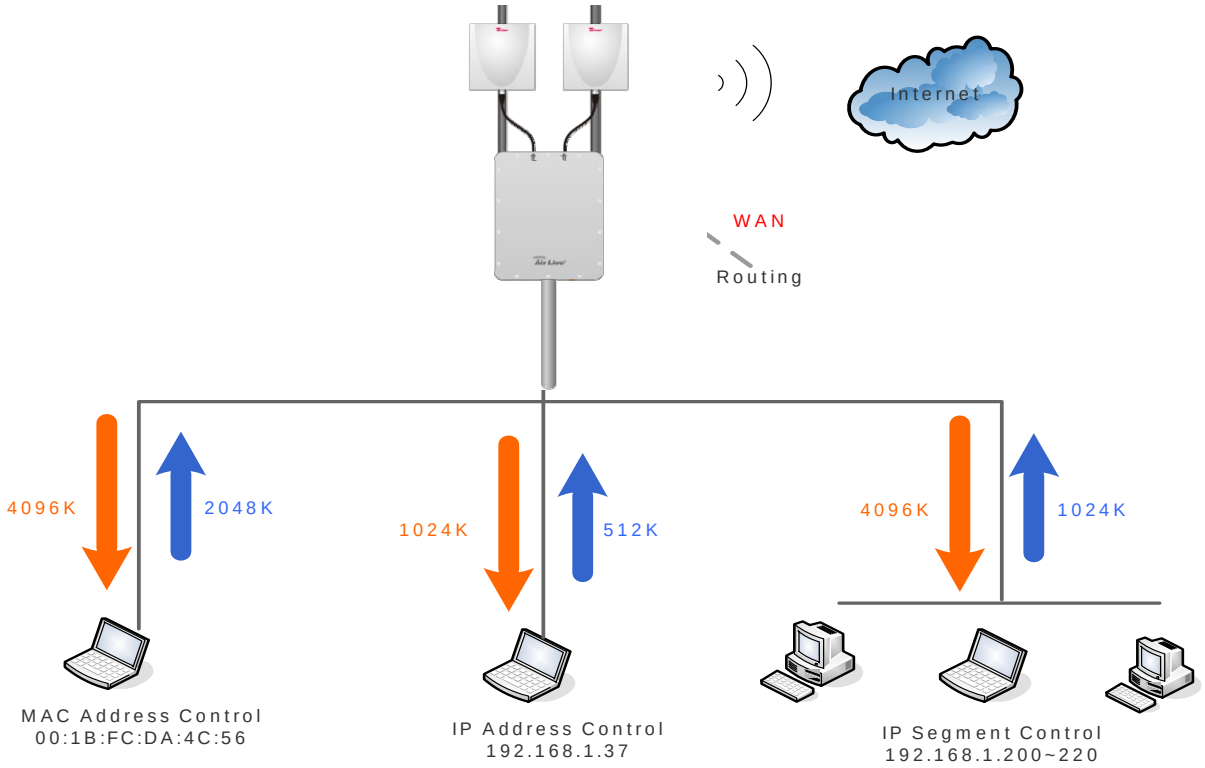
Example2:

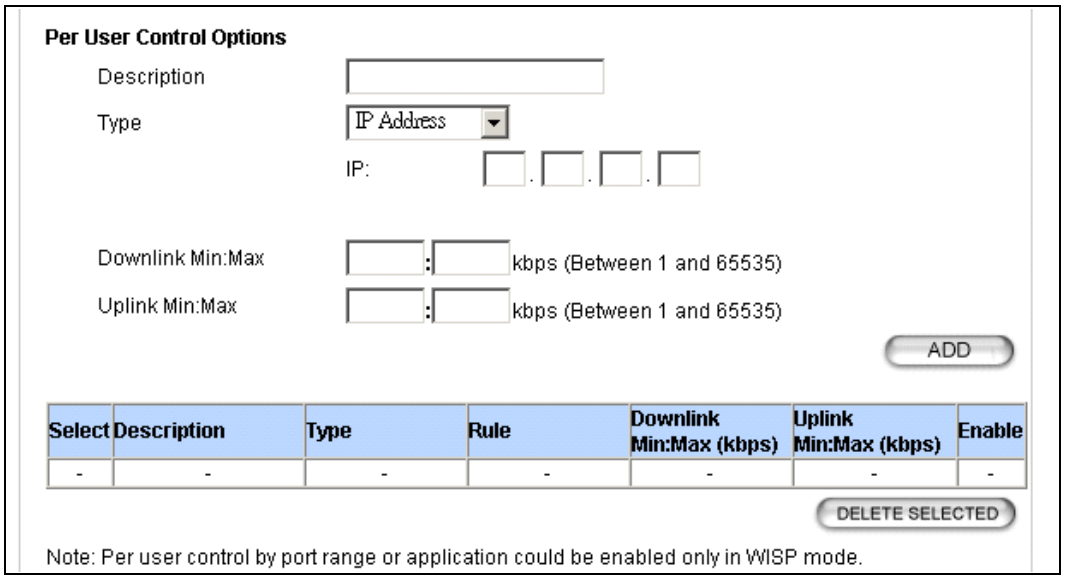
3 wired clients share downlink and uplink bandwidth.



In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

3.9.2 Per user Bandwidth Control

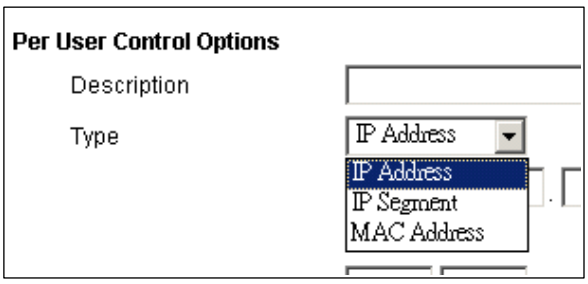




Note that this option could be enabled in WISP mode.

Description: You can preset your control type and named on the type.

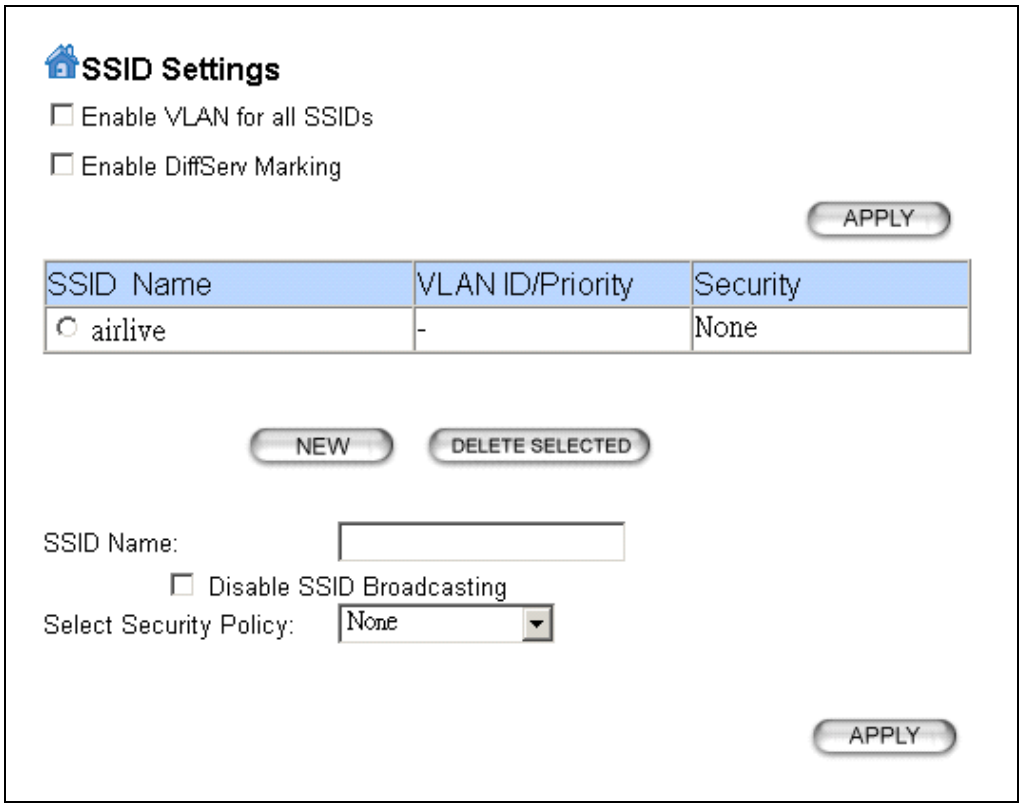
Type: Three types to be selected: IP Address, IP Segment and MAC Address. IP Segment allows you to set bandwidth limitation on an IP range.

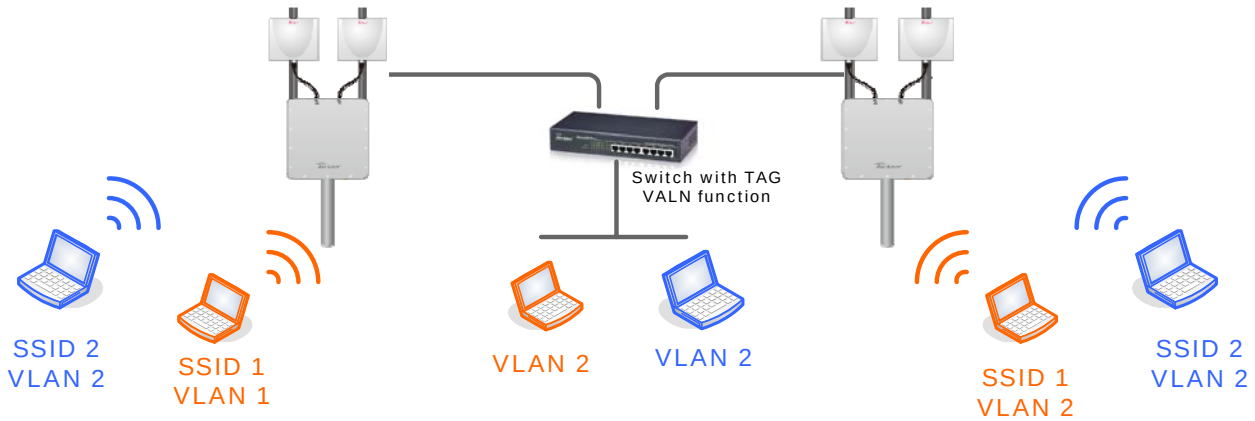


3.10 Multiple SSID + VLAN

You can configure up to 4 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. You can also assign VALN on each SSID to separate clients.

Note that the VLAN accept only tagged packet only.

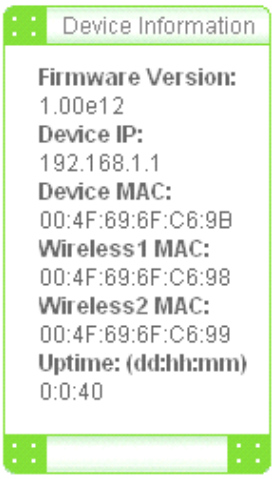




In the above example, laptops in VALN 1 can only communicate with those in VLAN 1 and laptops in VALN 2 can only communicate with those in VLAN 2.

4. System Management

You can review the Device information of your WH-9200AP by the interface. The information shows the current firmware version, IP address of your WH-9200AP.



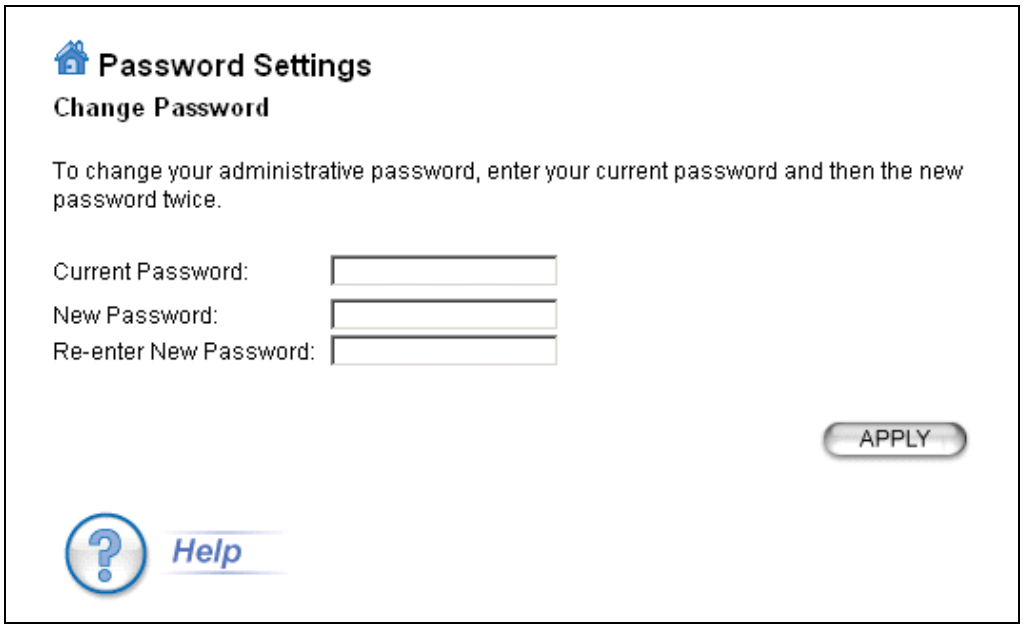
Wireless1 MAC and **Wireless2 MAC** show the MAC address of the two radios, the information helps to setup WDS connection by remote access point.

The **Uptime** records the live time of WH-9200AP after boot.

dd: day; **hh:** hour; **mm:** minute

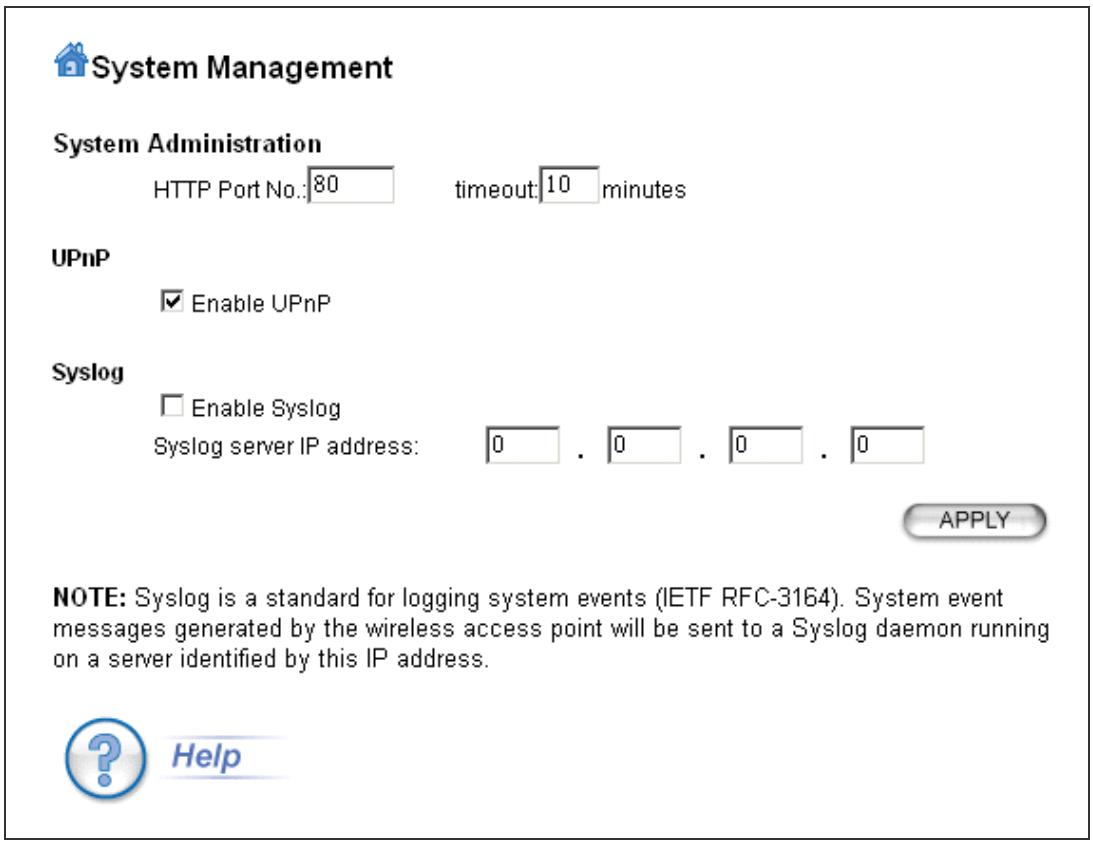
4.1 Change Password

It's recommended to set your own password instead of using default factory password. The default factory password is "**airlive**" all letters are in lower case. To change the password, press the **Password Settings** button to enter the **Password Settings** screen; then enter the Current Password followed by the New Password twice. The entered characters will appear as asterisks



4.2 System Management Settings

The WH-9200AP allow you to change the parameter of manage the system.


System Management
System Administration
HTTP Port No.: 80
timeout: 10 minutes
UPnP
Enable UPnP
Syslog
Enable Syslog
Syslog server IP address: 0 . 0 . 0 . 0
APPLY
NOTE: Syslog is a standard for logging system events (IETF RFC-3164). System event messages generated by the wireless access point will be sent to a Syslog daemon running on a server identified by this IP address.
Help

HTTP Port No.: This is to change the management web port of WH-9200AP. By default, the port number is 80 and we type http://192.168.1.1 in the browser to access the management web page. If we change the port to another, say, 90, then we need to type http://192.168.1.1:90 instead. This prevents unwelcome access to the management interface.

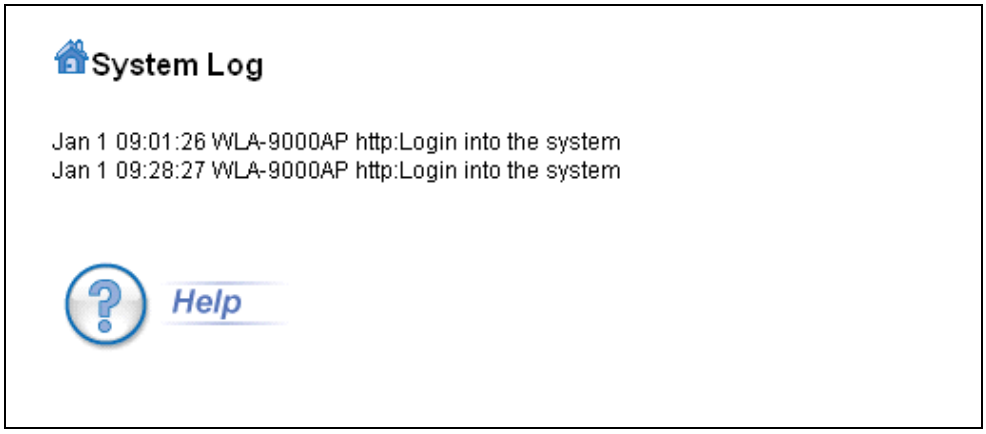
Time-out: The default is 10 minutes. If you idle on the web management interface more than 10 minutes, the system log you out and you need to login again.

UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this WH-9200AP and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).

Syslog: If the Syslog is Enabled, WH-9200AP create a log in the system log table when encounters an error or warning condition. This apply to IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164)

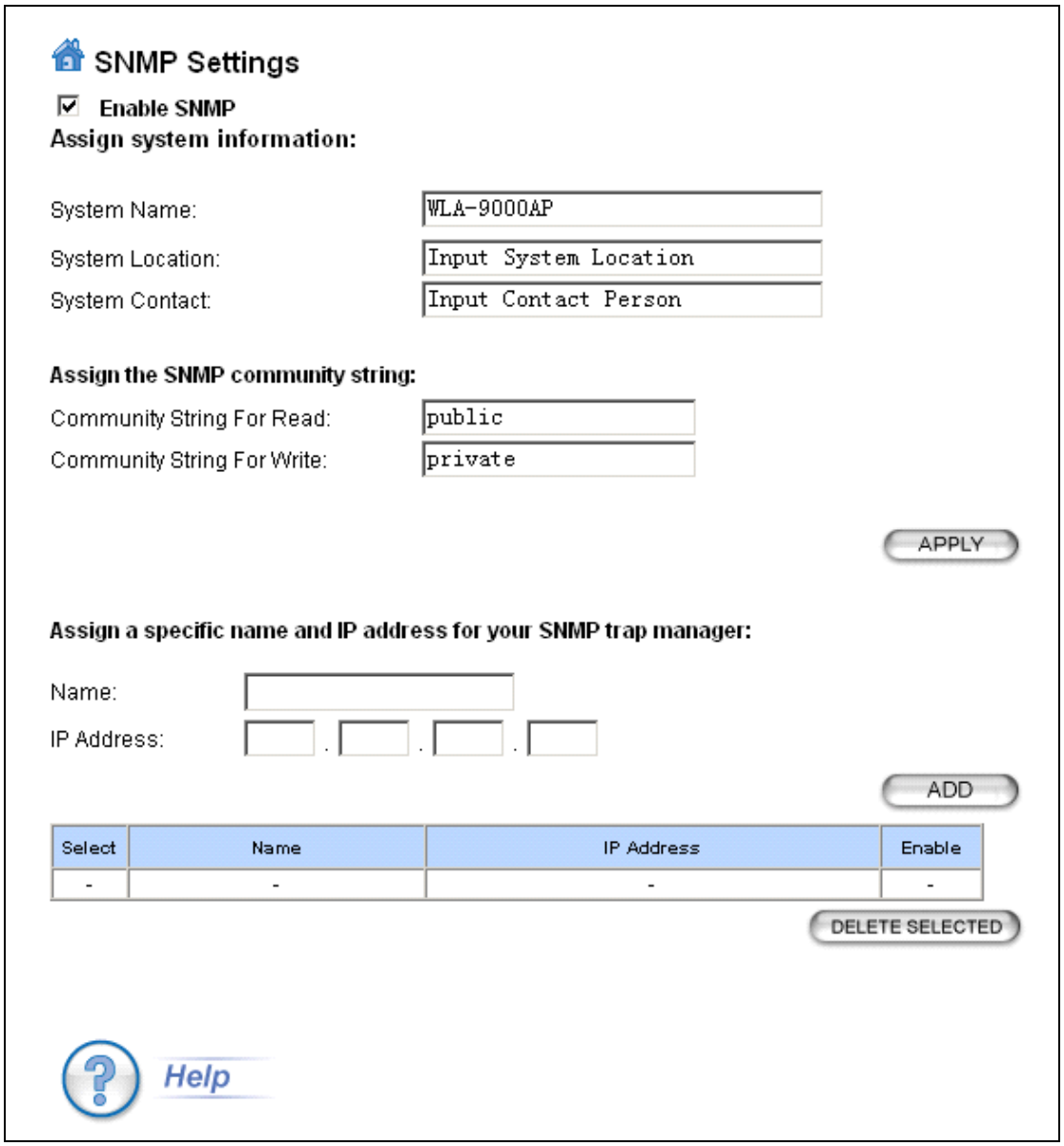
Syslog server IP address: The Syslog can also send to the identified IP address.

The system log shows in WH-9200AP:



4.3 SNMP Settings

WH-9200AP can also be managed by remote software with SNMP (simple network management protocol) protocol.



System Name: A name that you assign to your WH-9200AP for SNMP software. It is an alphanumeric string of up to 30 characters.

System Location: Enter a system location. Information for SNMP software.

System Contact: Contact information for the system administrator responsible for managing your WH-9200AP. It is an alphanumeric string of up to 60 characters.

Community String For Read: If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.

Community String For Write: For read-write operation, you need to configure a write “community string”.

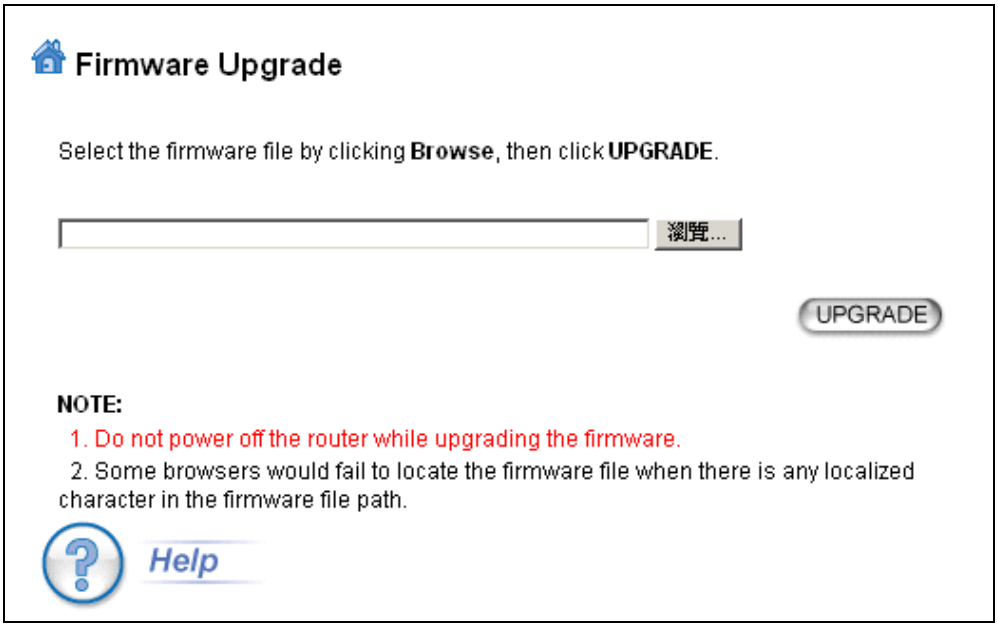
Assign a specific name and IP address for your SNMP trap manager:
A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.
You can define trap managers in the system.
You can add a trap manager by entering a **name**, an **IP address**, followed by pressing the **ADD** button.
You can delete a trap manager by selecting the corresponding entry and press the **DELETE SELECTED** button.

To enable a trap manager, check the **Enable** box in the corresponding entry; to disable it, un-check the **Enable** box.

Some extra feature of WH-9200AP does not show in the wizard because some higher knowledge of parameters of them is required. They are classified in the tab of “Advances Setting”, such as the Multi SSID for VLAN setting and 802.11e QoS configuration.

4.4 Firmware Upgrade

You can upgrade the firmware of your WH-9200AP (the software that controls your WH-9200AP's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version. System upgrade can be performed through the System Upgrade window as follows:


Firmware Upgrade
Select the firmware file by clicking Browse, then click UPGRADE.
瀏覽...
UPGRADE
NOTE:
1. Do not power off the router while upgrading the firmware.
2. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path.
Help

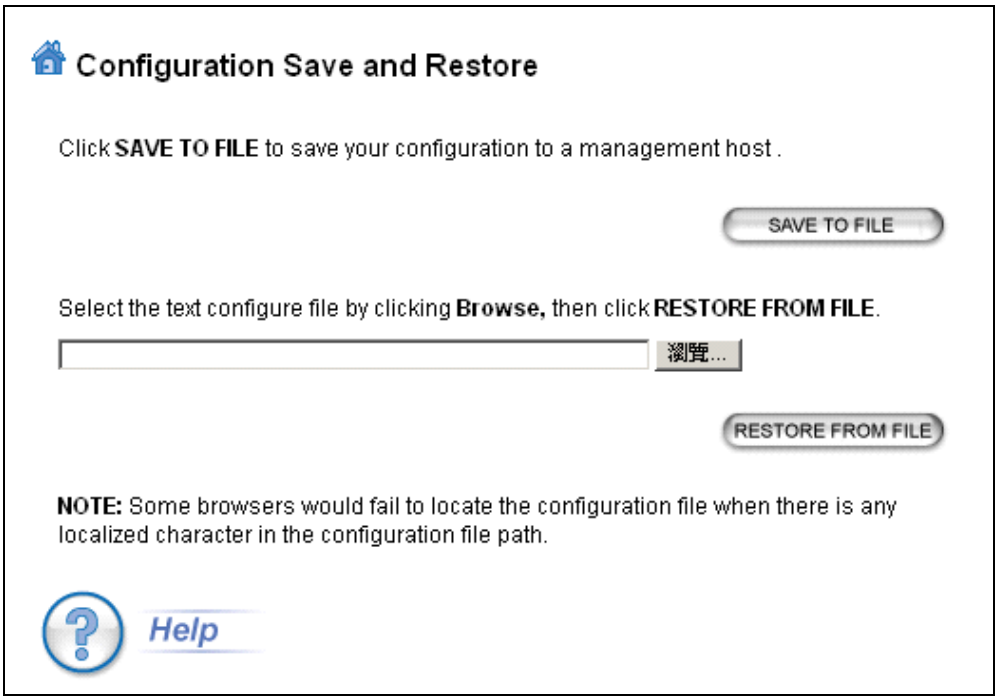
To update the WH-9200AP firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your WH-9200AP. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

Do not power off the device while upgrading the firmware.
It is recommended that you do not upgrade your WH-9200AP unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

4.5 Configuration Save and Restore

In this interface, you can backup your system configuration to PC and restore your saved configuration file to the WH-9200AP.

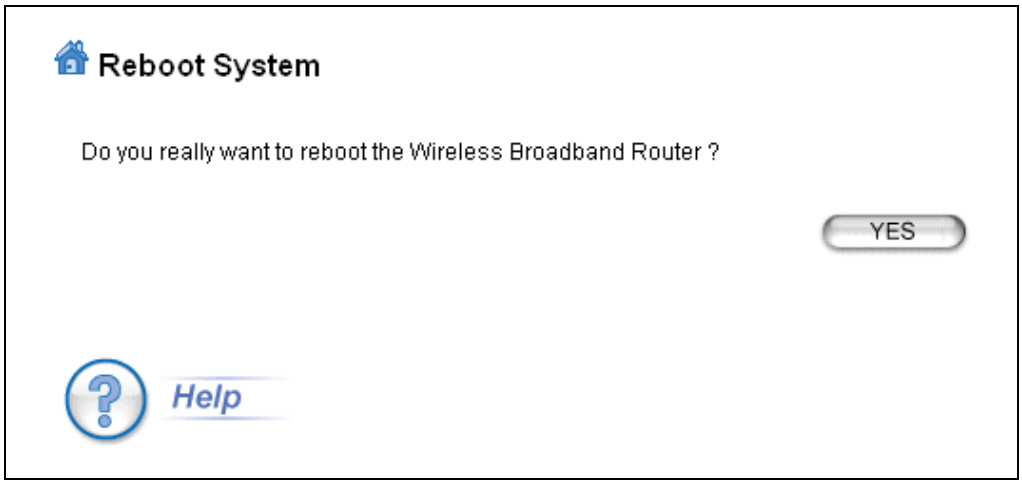

Configuration Save and Restore
Click SAVE TO FILE to save your configuration to a management host .
SAVE TO FILE
Select the text configure file by clicking Browse, then click RESTORE FROM FILE.
瀏覽...
RESTORE FROM FILE
NOTE: Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path.
Help

To save the configuration to your PC, click the **"SAVE TO FILE"** button and the system will lead you to save the configuration file to your PC.

To restore configure file to WH-9200AP, click the **"Browse"** button, find the saved configuration fire, then click **"RESTORE FROM FILE"** button to restore.

4.6 Reboot System

The following interface allows you to reboot your WH-9200AP. Click **"Yes"** button to reboot.

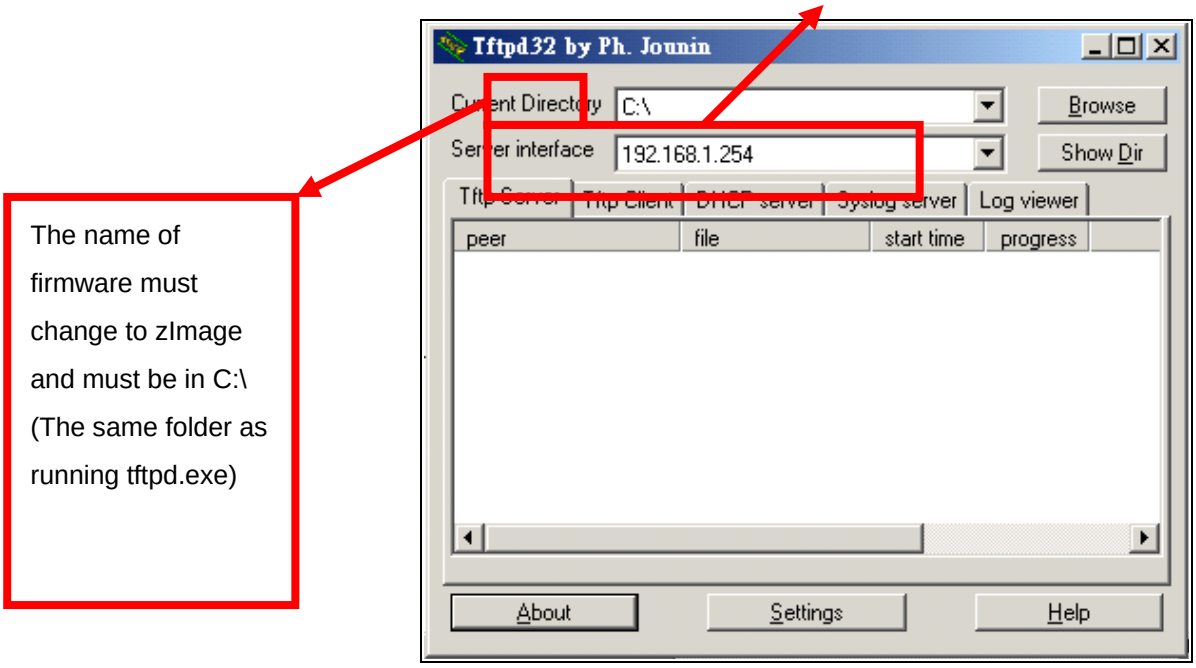


You can also reboot WH-9200AP by power off and power on it.

4.7 WH-9200AP Emergency Recovery

This document guides to recover your WH-9200AP system if the firmware crashed.

1. Download the tftp server to your PC. In the following example, we use tftpd32: http://tftpd32.jounin.net/tftpd32_download.html.
2. Copy the tftpd32.exe of the downloaded file to C:\.
3. Change the IP address of your PC to 192.168.1.254 / 255.255.255.0
4. Copy the WH-9200AP firmware to C:\ and rename the firmware to **"zImage"**. Note that the name must be zImage and no extension.
5. Connect WH-9200AP and PC with an Ethernet cable.
6. Run the tftpd32.exe. Note that the IP address must be 192.168.1.254.



7. Power on WH-9200AP, the **"Status"** LED will light on after 3 seconds.
8. Push the **"Reset"** button until the **"Status"** LED off and on again and release the **"Reset"** button.
9. If the above process success, the WH-9200AP LAN LED keep flashing and the tftp serve shows file download information.
10. It takes around 5 minutes to download firmware and around 5 minutes to update the firmware.
11. After a successful recovery, the WH-9200AP boots up automatically.
12. Try access 192.168.1.1, or the IP address you had changed before.
13. Repeat the processes again if failed.